

Die approbierte Originalversion dieser Diplom-/Masterarbeit ist an der Hauptbibliothek der Technischen Universität Wien aufgestellt (<http://www.ub.tuwien.ac.at>).

The approved original version of this diploma or master thesis is available at the main library of the Vienna University of Technology (<http://www.ub.tuwien.ac.at/englweb/>).



MASTERARBEIT

Evaluation of differences between optimization algorithms for the selection of IT and IT-security investments

Ausgeführt am Institut für
Softwaretechnik und interaktive Systeme
der Technischen Universität Wien,

unter der Anleitung von
o.Univ.Prof. Dipl.-Ing. Dr.techn. A min Tjoa

durch
Christian Hartl,
Rechte Bahngasse 10/2/23,
1030 Wien.

Wien, am 8. September 2007

Eidesstattliche Erklärung

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

Ort, Datum

Christian Hartl

Abstract

How much IT-(Security) is enough? Many valuation methods have been developed, which try to define the value of IT and IT security investments. As criteria like *Return on Investment (ROI)* can be seen as a concept with a set of methods, tools, activities, and ideas, there is still no guide on how to apply, and combine those methods in order to invest in the right *level* of IT-(security). This thesis aims to reduce the gap between IT and IT security investments in order to improve the 1) Estimation of input variables for IT security investments, 2) Alignment of IT security investments to the organization's objectives, 3) Valuation of IT investment alternatives considering the appropriate level of IT security investments. This is performed by the evaluation of differences between IT and IT security investments, resulting in a framework, which includes those advantages. This framework is shown in action by means of a case study. It shows 1) How Cost/Benefit Analysis, Real Option Valuation, Analytical Hierarchy Process, and Multi Objective Decision Support can be appropriately applied considering the categorization the IT investment into *low, medium, and high* risk IT investment 2) The advantages resulting of a process based valuation for IT security investments with Multi Objective Decision Support.

Kurzfassung

Wieviel IT-(Sicherheit) ist genug? Viele Bewertungsmodelle wurden entwickelt, welche versuchen den Wert von IT und IT-Sicherheit zu definieren. Da Kriterien, wie der *Return on Investment (ROI)*, als Konzept mit eine Reihe von Methoden, Werkzeugen, Aktivitäten und Ideen angesehen werden kann, gibt es noch immer keine Anleitung wie diese Modelle angewendet und kombiniert werden sollen, um in die richtige Höhe an IT-(Sicherheit) zu investieren. Diese These verfolgt das Ziel die Kluft zwischen IT und IT-Sicherheit zu reduzieren, um die 1) Abschätzung von Eingabewerten für Investitionen in IT-Sicherheit, 2) Ausrichtung von Investitionen in IT-Sicherheit an den Zielen der Organisation, 3) Bewertung von alternativen IT-Investitionen unter Berücksichtigung der geeigneten Investitionen in IT-Sicherheit, zu verbessern. Dies wird durch die Evaluierung der Unterschiede zwischen Investitionen in IT und IT-Sicherheit durchgeführt, woraus ein Framework resultiert, welches diese Vorteile inkludiert. Die Anwendung dieses Frameworks wird durch eine Fallstudie gezeigt. Sie zeigt 1) Wie Cost/Benefit Analysis, Real Option Valuation, Analytical Hierarchy Process, und Multi Objective Decision Support passend unter Berücksichtigung der Kategorisierung der alternativen IT Investitionen in *geringes, mittelmäßiges* und *hohes* Risiko, angewendet werden kann, und 2) Die Vorteile die aus einer prozess-basierten Bewertung mit Multi Objective Decision Support von Investitionen in IT-Sicherheit resultiert.

Contents

1	Introduction	7
1.1	Related Work/State of the Art	8
1.2	Research Questions/Approach	9
2	IT-Investments	11
2.1	Definition and Aim	11
2.2	The role of IT within an organization	13
2.3	IT and the business process	16
2.4	Planning IT Investments	17
2.5	Valuation of IT investments	19
2.6	Why measuring IT-Investments is hard	20
2.7	Summary	22
3	IT-Security Investments as part of IT-Investments	23
3.1	Definition and Aim	23
3.2	Planning IT-Security Investments	26
3.3	Valuation of IT-(Security) Investments	30
3.4	Why measuring Security-Investments is hard	31
3.4.1	Infinite Number of Things that can go wrong	32
3.4.2	Many Alternatives	32
3.4.3	Lack of Information	33
3.4.4	View on risks	34
3.4.5	Time Perspective	35
3.5	Summary	35
4	About Risks and Uncertainty: A Lack of Information	36
4.1	How Decisions are made	36
4.1.1	Representativeness	37
4.1.2	Availability	38
4.1.3	Adjustment and Anchoring	39
4.1.4	It won't happen to me	40
4.1.5	Out of sight out of mind	40
4.2	How Decisions should be made	41
4.2.1	... under Certainty	42
4.2.2	... under Risk	43
4.2.3	... under Uncertainty	47
4.3	Summary	48

5	Evaluation of IT-Investment valuation methods	49
5.1	Cost/Benefit Analysis	49
5.1.1	Sensitivity Analysis	51
5.2	Real Option Valuation	52
5.2.1	Uncertainty in the context of Real Options	52
5.2.2	Modification of the NPV	53
5.2.3	Real Option Calculation	54
5.3	Analytical Hierarchy Process (AHP)	56
5.4	Multiobjective Decision Support for IT investments	59
5.5	Summary	61
6	Evaluation of IT-Security Investment valuation methods	62
6.1	Defense trees for economic evaluation of security investments	62
6.2	Mizzi's Return on Information Security Investment	65
6.3	Security Attribute Evaluation Method	69
6.4	Multiobjective Decision Support in IT-Risk Management	72
6.5	Summary	76
7	Case Study for IT (security) investments	77
7.1	The Business Case	77
7.2	IT investment alternatives	80
7.3	Cost/Benefit Analysis	83
7.4	Real Option Valuation	85
7.4.1	Calculating Real Options	88
7.5	Multi Objective Decision Support	91
7.6	AHP Analytic Hierarchy Process	92
7.7	Multi-Objective Security Safeguard Selection Tool	95
7.8	Summary	99
8	Elaboration on Research Questions	100
9	Conclusion	108
	Acknowledgements	109
	References	110
	List of Figures	119
	List of Tables	120
	Appendix A - Real Options Calculator	121

Appendix B - AHP Calculator	122
Appendix C - MODS Calculator	124
Appendix D - MOST Get portfolio value	127

1 Introduction

Whereas, assessing the return on investment has always been a stumbling block for regular technology investments, assessing the return on investment for IT-Security investments seems to be more challenging. In contrast to IT investments, IT-Security investments reduce the cost of security breaches [1]. Researchers (e.g. [20], [21]) agree that due to the increasing interconnectivity and complexity of IT-Systems, the likelihood of IT-Security breaches increases. Every new product that is introduced on to the IT market, adds a new security twist. The threats are more sophisticated, and the attacks more numerous. According to the survey 2006 of the *Information Week* [47] forty-eight percent of the over two thousand security professionals and business technology managers who completed the survey say that managing complexity of security is their top challenge.

The *Computer Emergency Response Team* (CERT) evaluated that the number of security breaches increases exponentially so do their costs. The 2004 CSI/FBI Computer Crime and Security Survey revealed that the overall financial losses totaled from 494 survey respondents were \$141,496,560. Based on responses from the 494 computer security practitioners in U.S.corporations, government agencies, financial institutions, medical institutions and universities, the findings of this survey verify that the threat from computer crime and other information security breaches is existent. The *Information Week* [47] revealed in their survey 2006 that fifty-seven percent of U.S companies were hit by viruses in the past year, thirty-four percent by worms, eighteen percent by denial-of-service attacks, nine percent by network attacks and eight percent by ID theft attacks.

Cavusoglu et al. [22] used an event-study analysis, using market valuations, to assess the influence of security breaches on the market value of breached firms. The results of their study show, that the breached firms lost 21 percent of their market value within two days after the announcement. In addition they determined an average loss in market capitalization of \$1,65 billion per incident. They evaluated effects for security developers, as well. The market value of security developers is positively related with the disclosure of security breaches by other organizations. They came to the point, that the cost of poor security is very high for investors. This study leads to the insight, that the returns of an IT security investment can affect the organizations strategic drivers, like the *Brand Name*. Therefore IT security investments have to be seen within the organization's strategy. Undoubtedly these studies show the importance of research on the economics and management of IT and IT-Security investments.

1.1 Related Work/State of the Art

IT investments are directly linked to business processes [70] [74]. Viewing IT from this process perspective leads to a well established measurement of the business value of IT [70]. IT investments may contribute to overall organizational performance by further improving the financial performance, and strategic performance [85]. In order to measure the effect of IT on the overall organizational performance, valuation methods like *Cost Benefit Analysis*, *Real Option Valuation*, *Analytical Hierarchy Process*, and *Multi Objective Decision Support* may be used. Nevertheless, organizations then to apply only one single criterion, which does not catch the consideration of the organization's objectives in the valuation of IT investment alternatives.

In addition Mooney et al. [70] states, that organizations derive business value of IT from two sides: 1) through its impacts on intermediate business processes, and 2) through redesigning current business processes. Early studies (e.g. [38], [28]) propose the categorization of IT investments into *low*, *medium*, and *high* risk IT investments. This categorization basically depends on if current business processes are changed (high risk IT investment), or if current business processes are boosted up by IT (low risk IT investments).

In contrast, the return of IT security investments are not valued in a comparable process oriented view. Qualitative methods, or so called frameworks [73], like they are proposed by the Bundesamt Sicherheit [105], Department of Defense [107], and Common Criteria [106] offer extensive guidelines to test/implement *security levels* of an IT system. Raz et al. [80] performed a comparison between qualitative standards. The authors came to the point that those standards are quite similar. The major difference between those standards is the different usage of terminology. So a discussion between those standards is quite difficult, because those standards define for example risk very different.

Such qualitative approaches offer technical guidelines, but they do not elaborate on the question "What *level* of security is enough?". This question can be answered by quantitative methods, or so called valuation models [73], which aim to value the return of a security investment. In literature there are a lot of valuation models to find (e.g. [84], [90], [92], [14], [86], [75], [69]), which offer mathematical models to calculate the value of IT security investments.

Both fields are facing the challenge of dealing with risks, and uncertainty about future outcomes, which results in the problem of estimating input values for their valuation models. The question, which arises from this problem is problem is "What do we do if probabilities are unknown or irrelevant?". Jablonowski [55] addresses this issue, and comes to the point, that it is necessary to do a more thorough study of decision methods under conditions where probability information is limited, or of limited value.

There are two ways to improve this decision making process: 1) Improve managemen-

t/process of (subjective) estimations, and 2) Aligning the investment to the organization's strategic drivers. The more promising way seems to be to reduce the gap between IT and IT security investments (cf. [21], [55], [29]).

An early idea to improve the decision making process for IT security investments is proposed by Neubauer et al. [73], who took the second solution strategy under consideration. The authors propose a framework, which connects the cost-benefit valuation of security with business processes. This approach focuses on this challenge by improving the valuation of IT security, which results in better data collection and analysis according to changing requirement of the corporate business processes. Researchers (e.g. [72]) refined this approach, by applying the Multi-Objective Safeguard Selection Tool (MOST) [75] for the process based valuation of IT security investments. This approach offers the possibility to value the right *level* of IT security investments under consideration of the organization's strategic drivers. This thesis is based on these ideas, and will further improve the estimation of input variables by establishing a connection between IT and IT security investments.

1.2 Research Questions/Approach

"Communication gaps between security managers and IT managers have been often reported" [29], resulting in a technology-centric view on IT security, which does not catch the organization's strategic drivers [21]. This thesis aims to reduce the gap between IT and IT security investments, to improve the decision making process for IT and IT security investments by answering the following research questions:

- What are the differences between IT and IT security investments? This question will be answered by evaluating both fields under the following criteria:
 - Definition
 - Aim
 - Planning
 - Challenges
- What processes, from a psychological point of view, influence in what way the result of a subjective estimation of input variables? This question will be answered through theoretical research.
- What are the differences between valuation methods of both fields? This question will be answered by evaluating the following valuation methods: Cost/Benefit Analysis, Analytical Hierarchy Process (AHP), Real Option Valuation (ROV), and a Multi Objective Decision Support System (MODS) for IT investments, and Mizzi's Return on Security Investments, Defense Trees, Security Attribute Evaluation Method,

and Multi-Objective Safeguard Selection Tool (MOST) for IT security investments. Those methods will be evaluated under the following criteria:

- Type: Financial Technique/Operations Management technique.
- Which challenges are addressed?
- How the challenges are solved?
 - * Input/Output variables: This criterion evaluates the Input and Output Variables of the methodologies. This will show 1) how the challenges are understood in both fields and 2) if/how methodologies can be combined for both fields.
- Advantages/Disadvantages? This criterion will evaluate the Advantages/Disadvantages of the methodologies, by 1) contrasting researchers opinions and 2) Deriving from how challenges are understood and solved.

The aim of this evaluation is to develop a framework, where IT investment alternatives can be valuated, considering the investment of an appropriate level of IT security alternatives. In addition this framework will improve the decision making process by focusing on the problems: 1) Missing guide for IT investments [30], 2) Improve the estimation of input variables for IT security investments, by aligning them to the IT investment, with a process based approach. This framework will be shown in action by means of a case study.

2 IT-Investments

This section focuses on the definition of IT investments. It will introduce IT investments under the aspects: *definition*, *aim*, *planning steps* and *challenges*. Further this section introduces the *Risk Management Process* for IT investments. It aims to give an understanding from which sides the return of an IT investment comes from, and how it can be valuated.

2.1 Definition and Aim

Investment is a term used in economics, which has to associate senses: The first one is the acquirement of financial assets with the purpose to get capital gains. The second one relates to the creation of productive assets, which may be called *fixed investment* like buildings or equipment. Those two senses can be connected. For example when a company invests in shares and uses the money to build a new factory. In ordinary speech the term investment is even more widely used: people invest in works of art, cars, and even in furnishings [108]. Those usages of investment have in common that one puts an effort in something from which he expects an (in)direct benefit.

In the crystal encyclopedia [108] a broad definition of information technology can be found. It is important to add, IT differs from *technology*. While technology is referred is a broad term, which can be applied to the use of knowledge of tools and crafts to produce products and solve problems, information technology (IT) is related to technology, and to the different aspects of managing and processing information [81]. This definition is similar to the definition, which can be found in the crystal encyclopedia. Information technology is used to cover the range of technologies relevant to the transfer of information (knowledge, data, text, drawings, etc), in particular to computers, digital electronics, and telecommunications [108]. But for this thesis there is the need of a definition which relates stronger to economics. Such a definition can be found in the Executive Guide for Information Technology Investment Management from the General Accounting Office [104]:

Information Technology (IT): The computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources used by an organization to accomplish a function [104].

This definition implicates two major components related to Information Technology: *Hardware* and *Software*. Those components can be summed to define the term *IT-System*. But this definition does not catch the complexity and extensibility of nowadays IT systems. The following definition of IT investment implicates those two aspects by referring an IT system to components which are connected together in order to facilitate the flow of information [108].

IT Investment can be defined as the decision by an organization to expend resources or the actual expenditure of resources on selected information technology or IT-related initiatives with the expectation that the benefits from the expenditure exceeds the value of the resources expended [104].

Why do organizations invest in Information Technology? The major *aim* is a positive relationship between spending on information technology (IT) and resulting benefits to productivity or effectiveness [85]. This positive relationship is referred to the *Return on Investment (ROI)*, which can be defined with the following equation:

$$ROI = \frac{Benefits}{Costs} \quad (1)$$

In its most basic economic sense, a cost is whatever you have to give up, and a benefit is anything good that you get as a result, whether that good is measured in tangible or intangible terms [30]. This simple definition of ROI, should not lead to the insight, that calculating the Return on an IT investment is an easy duty. In fact, ROI in IT is referred to tangible benefits, costs, and risks. In particular, intangible benefits, costs, and risks can be the most important factors to valuate an IT investment, but they are challenging to quantify and to measure [81]. This is the reason, why many approaches exist to valuate the ROI for IT. There is no guide on how to perform a ROI valuation for IT investments. How to approach a ROI valuation typically depends on the situation in which an IT investment is valuated. According to Cresswell [30] ROI is not just a single component. Instead, he understands Return on Investment for IT-Investments as a set of methods, tools, activities, and ideas. They can be combined and used in many different ways to judge the value of an investment over time. Therefore choosing the right tools for a ROI analysis will usually depend on a number of factors. There is no strict combination of methods to find for valuing an IT investment. Due to this reason authors like Cresswell [30] or Pobbig [79] see ROI as concept, which has to be framed in the organization's specific situation.

However, it is essential for a ROI valuation to understand from where costs and returns come from. This makes it necessary to take a closer look on the organization's objectives, and the role IT takes within the organization, in order to achieve those objectives.

2.2 The role of IT within an organization

On top, an organization can be viewed as a *black box*, which generates an output (products, services) from an input (raw materials, manpower), which are typically expressed in monetary units. The amount and types of inputs, and outputs differs from organization to organization. Elaborating on the different kinds of inputs, and outputs would exceed the scope of this thesis. Therefore it sees those inputs, and outputs only in the sense of monetary units.

Costs, and returns of an IT investment can derive from an organization's technology infrastructure, business processes, environment, and external relationships [30], due to their alteration which is caused by new IT. An IT investment directly changes technology systems, which are already in place. This may change the way the efficiency of automation, and workflow of the current IT infrastructure.

The IT infrastructure, and therefore the IT investment, is directly linked to the business process. IT systems automate these processes, which results in achieving the organization's objectives more efficient.

Business Process as a collection of related structured activities-a chain of events-that produce a specific service or product for a particular customer or customers [30].

Business Processes are linked to the organizational environment. The change of current business processes may have effects resource flows, performance changes, changes in work flows and internal relationships. For example the change of a static HTML based website to a dynamic XML based website, would typically change the way on how new information is added, structural modifications are performed,... This would change the tasks of the employees leading to altered workflows.

This change may have effects on the external environment of an organization. Sticking to the previous example, the change from a HTML based website to a XML based would create new services. For example the representation of the website could be linked to the customer's preferences. Despite this aspect of the relation to external persons, and new persons, changes of the external environment can result in new ways business is performed with other organizations. For example a new database can change the way business is conducted with the organization's suppliers. This view is shown in figure 1.

On the way to evaluate the benefit and costs of an IT investment, the decision maker has to consider risks, which are related to these organizational levels.

Risk can be defined as the combination of the probability of an event and its consequences [103].

Although risks can be viewed as possible events that constitute opportunities for benefits, and threats that lead to costs, risks are mostly referred to losses in risk management.

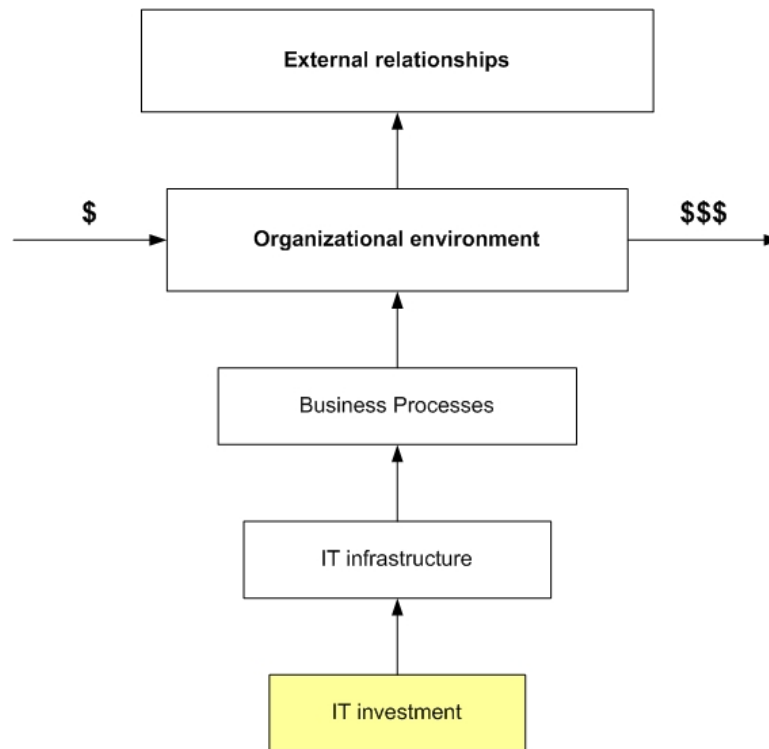


Figure 1: IT investment relations

For example Cresswell [30] subsumes risks into the following categories, which derived from the above organizational levels:

- *Politics and policy risk factors.* Examples for environmental risk factors include multiple stakeholders, and their changing demands. Another example can be changing market developments.
- *Organizational risk factors.* Examples for organizational risk factors include organizational acceptance of IT, like user acceptance. So the organization must support their employees in adopting to changing demands.
- *Business process risk factors.* Business process risks reflect themselves in missing flexibility to changing demands, or the missing support of business needs.
- *Technology risk factors.* Technology risk factors are referred to technology interactions, when new technologies interact with old ones, or they are referred to the rapid changes of technology. This changes can lead to the difficulty of understanding how the new technical tool works, or they make it difficult for planners to keep up with the details of new developments [30].

The author uses the categorization "Politics, and policy risk factors", because his discussion focuses on IT investments for governmental constitutions. The difference to other organizations is, that they do public business, and are therefore stronger influenced

by legislators, executive officials, and the public, than other organizations. However, the basic concept of this risk categorization is adoptable for every organization. Therefore it is more appropriate for this thesis to call this classification "Environmental risk factors".

The previous examples catch only a small amount of possible risks, which can affect an IT investment. The process that supports the decision maker to deal with risks is called *Risk Management*

Risk management is the identification, analysis and treatment of an economic entity's exposures to loss [27].

In order to put this definition to its simplest: "It is the management of risks". This process is not unique for IT investments. In fact, risk management is a fast developing discipline with many views and descriptions of what risk management involves, how it should be applied, and what objectives are considered [103]. People even face this process in many areas of their daily life. For example many people invest in a safe where they keep their worthy goods. Most probably, they have weighted the cost of those investments to the value of their goods which they want to protect. According to Bistarelli et al. [14] "the risk management process is a fundamental activity in an enterprise, because it helps senior managers to make good decisions, based on protecting the organization and its ability to achieve its mission." Literature offers extensive guidebooks for risk management (c.f. [33]). A detailed discussion of the risk management would at this point exceed the scope of this thesis. Section 3.2 will go into further detail of the risk management process with special focus on IT security.

It is important to add, that risk management is a continuous and developing process, which implements the organization's strategy. It translates the strategy into tactical and operational objectives [103], which makes clear, that it is essential to align an IT investment to the organization's objectives, because it supports the more efficient valuation of costs, benefits, and risks associated with the IT investment.

Costs and benefits are sometimes subsumed under the term *Business value of IT*. It may be defined as the overall value of IT for a particular organization. Assessing business value of IT provides insights into the effects IT investments have on the bottom line performance of an organization [85]. Schniederjans [85] subsumes the effects of IT investments under the improvement of: 1) financial performance 2) business performance, and/or 3) strategic performance

Elaborating on all aspects, where costs and returns come from, would exceed the scope of this thesis. This section just introduced the variety of aspects, which have to be considered in a ROI analysis (cf. Cresswell [30] for further details). This thesis will focus on the relation of IT investments to the business processes, which will be discussed in the following section.

2.3 IT and the business process

Too often, companies design their IT strategies around what they are currently doing (existing assets, programs, and capabilities) and fail to focus on what they could be doing [28].

This statement leads to the importance of a business process analysis, and their relation to an IT investment. IT can have a direct impact on a business process, or on other related business processes. For example adding a new section on a web site could have serious effects on the demand, which can make it necessary to add additional server capacity. The important role of a business process analysis lies within their relation to the overall strategic objectives of an organization [30]. This aspect is supported by Mooney et al. [70]. They state that it is important to move to the process level in order to understand the role of IT, and the potential to enhance the organization's process and structure.

Besides the definition of a business process presented in the previous section Mooney et al. [70] propose the following definition: "specific ordering of work activities across time and place, with a beginning, an end, and clearly identified inputs and outputs". They further divide business process into operational and management processes. While management processes are referred to administration, allocation, and control of resources, operational processes are related to the execution of tasks. For example e-mail, or video-conferencing typically support management processes. On the other side robotics, and workflow systems support operational processes.

This differentiation can be further divided into marketing and intelligence processes, design and development processes, procurement and logistic processes, production processes, product/service delivery processes, information handling processes, coordination processes, control processes, communication processes, and knowledge processes [70]. Those business processes and their relation are illustrated in figure 2. This shows the direct impact of IT on various business processes, and the complexity a decision maker has to face.

This figure illustrates that IT on the other side generates processes. It gives an idea of the complexity, which a decision maker has to face, when he has to value an IT investment. Note that dependencies between those processes are not considered at this point.

Changing the way on how business processes are executed is referred to the term *Business Process Re-engineering* [70]. This plays a critical role in order to maximize the return of an IT investment. "Fundamental rethinking and radical redesign of an entire business system ... to achieve dramatic improvements in critical measures of performance.[31]". There are many ways to optimize the business process allocation. Cresswell [30] subsumes approaches to process modelling in descriptive, analytical, and dynamic models (cf. Cresswell [30], Schniederjans [85] for further details).

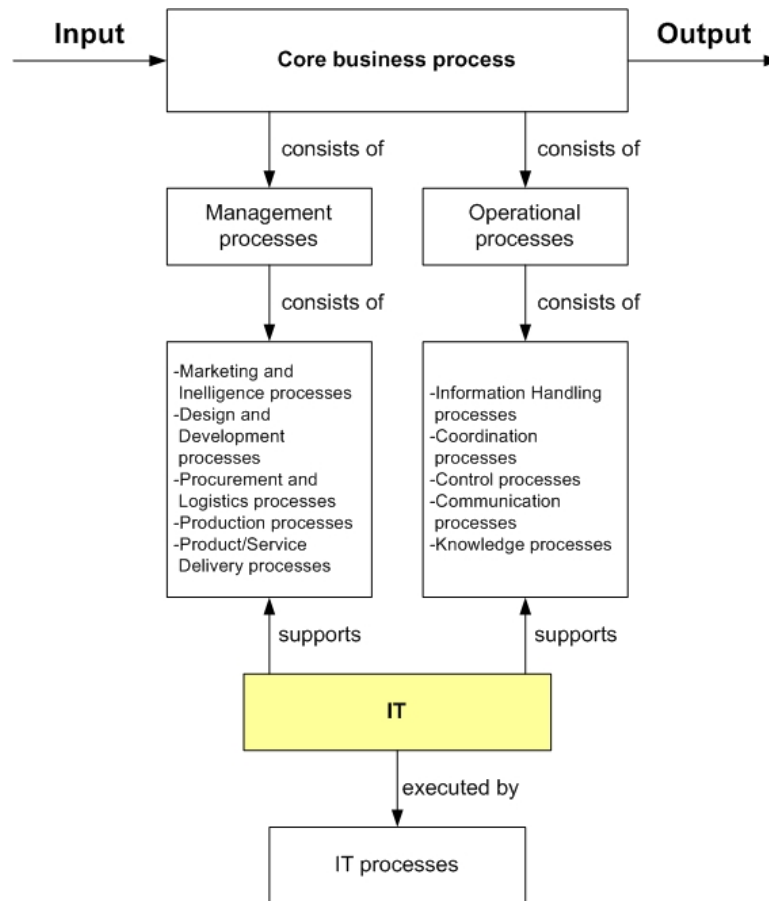


Figure 2: Business processes

2.4 Planning IT Investments

This section elaborates on a *formal* way to plan an IT investment. The aim of this section is to show the planning steps, where valuation methods for IT investments are applied. Schniederjans [85] proposes three steps:

1. *Strategic plan*: It includes the analysis of competition and threats, the analysis organization's strengths and weaknesses, and the overall corporate strategic planning, which results in the organization's objectives.
2. *Tactical plan*: It includes process and systems engineering, configuration and functionality analysis, and IT system evaluation and justification, which results in the choice of the *best* IT investment alternative(s).
3. *Operational plan*: It includes IT system implementation, and post implementation analysis, which will be of no further concern in this thesis.

These Planning steps and their relation to the introduced effects of an IT investment of figure 1 are shown in figure 3.

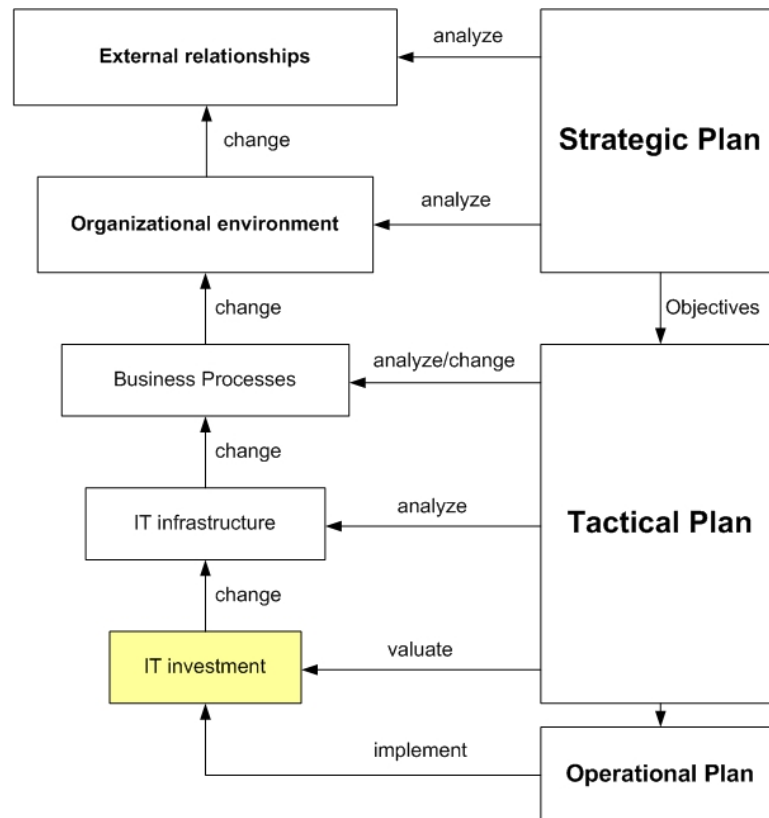


Figure 3: Planning steps

These planning steps show, that those are normally performed by different persons/management levels. This thesis will focus on the Tactical planning steps, because the other steps perform a broader analysis, which would exceed the scope of this thesis.

The needs analysis determines what technology, software, human resources are necessary to realize the organization's strategic objectives. It evaluates an IT investment by 1) a current status or capacity of the organization's IT, and 2) future needs that define what new or additional requirements, which are necessary to achieve the organization's strategic objectives. Cost assessments are necessary in the first three steps of the tactical planning process [85].

In the second step of *IT investments* we have to develop alternatives in order to compare them with each other. The simplest alternative for one given IT investment is to ask what are the costs and returns when we use the existing system without a change: Continuing with the present system with little or no change assumes the present technology is adequate for present and future requirements. In contrast if the present system is not adequate in functionality, processing capacity, then this strategy may be inappropriate. There are many possibilities for alternative generation. For example it is possible to evaluate the effects of upgrading the existing system. Minor or major system changes with a series of upgrades of modules can allow a less costly and less potential disruption to a system compared to a new one [85]. In particular decision makers can generate different solutions

for specific parts of the business process. Those alternatives have to be valued with IT investment methodologies in order to choose the alternative with the highest return on investment.

2.5 Valuation of IT investments

For the valuation of IT investment a lot of methods exist. Schniederjans [85] introduces a variety of methodologies for the valuation of IT investments, which can be framed in two major groups: 1) Financial Techniques and 2) Operations Research/Management Science Techniques [85].

1. Financial Techniques: examples: Accounting Rate of Return, Break even Analysis, Cost Benefit Analysis, Cost Benefit Ratio, Cost Revenue Analysis, Internal Rate of Return, Net Present Value Analysis, Payback Period, Profitability Index, Return on Investment.
2. Operations Research/Management Science Techniques: Optimization Methods examples include: Decision/Bayesian Analysis [46], Delphi Evidence [98], Game Playing [61], Multi-objective/Multi-Criteria Approaches [74], Simulation [17], Cost-Value Approaches [58].

In addition Schniederjans [85] defines categories like "Techniques Specifically Designed for IT Investment decision making", where he lists modified methodologies which are based on methods from above. For example: Cost-Value Approaches [58], Automatic Value Points, Buss's Method, Return on Management, . . . and "Other Techniques" in which he categorizes *new* methods of left over decision making methodologies like "Real Options Valuation" and the "Balanced Scorecard Method." For this thesis only the first two categories are used, because the methodologies mentioned in 3 and 4 can be put in section 1 and 2. For example AHP and Balanced Scorecard Method are Cost-Value approaches (e.g. [58]).

2.6 Why measuring IT-Investments is hard

It is possible to divide challenges into two parts: 1) Optimizing business processes according to the organization's strategic drivers (Strategic Plan, Tactical Plan) 2) Valuation of IT investment alternatives (Tactical Plan). For example Appel et al. [8] performed a study which revealed that IT investments do not correlate meaningfully with financial returns. There were only 50 out of 94 companies, which got returns due to their IT investments. This finding implicates there was a lot overspend in IT the past decades due to the following reasons, which relate to the first point:

1. Organizations spend in IT, without considering the productivity levers [38]. "Up to 60 percent of IT investments depend on its market position and aspirations." [28]
2. Organizations do not consider sequence and timing of IT investments [38]
3. Organizations see IT as a black box that generates costs [7]. variable/fixed costs, tangible/intangible costs
4. "IT investments often do not fully support the business needs." [74] Especially they are too expensive, and not flexible enough to adapt themselves to changing demands [30].

Organizations today are very careful when they think about an IT investment, because there was a lot overspent in the past decades (c.f. [7] [38]). It is necessary to improve the choosing and managing of IT investments. On this way it is necessary to focus on the challenges for valuating IT investment alternatives in this field: 1) "Existing business process management approaches do not integrate methods for evaluating and selecting efficient IT investments." [74] 2) "More sophisticated approaches like Real Options confront decision makers with complexity that causes scepticism." [74] 3) "Many valuation methods aggregate all benefits to a single value." [74]. For example: Net Present Value

For challenges derived from type 1 the McKinsey Global Institute (MGI) [38] propose to differentiate between kinds of IT investment (or Innovation). From this categorization follow two priorities: 1) Identification of the productivity levers with the greatest opportunity for competitive differentiation. The difficulty lies within the understanding of the complex factors that drive economics of individual companies and the way IT can influence those key factors. 2) Sequence and timing of investment. Many technology based advantages, especially those of kind 2, have a limited life. Timing is therefore important to get returns out of the IT investment.

But for companies that are unlikely to match in all productivity levers, where technology is widely available the right way is to implement standard off-the-shelf applications. On the other side customization makes sense when the IT investment catches lasting advantages [38].

Studies (e.g. [38], [28]) show that organizations that invested in IT successfully divided their investments into high, medium and low risk investments. Therefore Craig [28] goes one step further and proposes three kinds of IT investments and their related risk of the investment:

1. *Scale IT investment* Such IT investments reduce operational costs or ensure service and quality levels. (low risk investments).
2. *Competitive-advantage investments* Those IT investments increase the effectiveness of decision making or the efficiency of operations. Often those IT investments are combined with other business and operational investments. (medium risk investments).
3. *Rule-changing innovations* They deliver competitive advantage by creating new products/services, by generating "hard-to-replicate" cost or performance advantage. They focus on changing the race within a sector. (high risk investment).

He proposes to base portfolios on those categories. Organizations focus often on "stay-in-the-race" that are realized through "Scale IT investments" often miss out on IT investments (of type 2 or 3) that could help to deliver the strategic competitive advantage. By distinguishing among those categories organizations can use IT systems for *top-line* growth and market advantages [28].

2.7 Summary

This section showed, that IT investments are related to a very extensive field, because IT affects many areas of an organization. It described IT investments under Definition, Aim, Planning, and Challenges. It showed the relation of an IT investment to business processes, organizational environment, and external relationships. Challenges in this field derive from two sides: 1) Optimizing business processes 2) Aligning/Valuating IT investment alternatives according to the organization's strategic drivers.

In order to manage the first challenge extensive analysis of the organization is necessary. How this analysis is performed depends on the specific situation of the organization (External relationships, market, structure,...). This analysis results in tangible/intangible costs/returns and risks. Therefore there is no guide on how this analysis should be performed. Studies suggest to categorize the resulting IT investment alternatives into low, medium, and high risk IT investments. The difference within this categorization stems from altering existing business processes. If the IT investment just boosts up the existing business process, it would be characterized as a low risk IT investment, because their influence on the structure of the organization, and the resulting effects on the organizational environment and external relationships would be minimal. In this case, the amount of risks, stemming from those scopes, would be low. If on the other hand the IT investment changes the structure of existing business processes, the IT investment would have effects on those scopes, which results larger amount of risks, which can be understood as intangible costs and returns for the valuation of IT investment alternatives.

This results in a high demand on valuation methods for IT investments, which have to consider this complexity. This stands for process based valuation methods of IT investments, which catches this complexity, by aligning the valuation to the organization's objectives.

3 IT-Security Investments as part of IT-Investments

This section focuses on the definition of IT security investments. It will introduce IT security investments under the aspects: *definition, aim, planning steps* and *challenges*. Further this section introduces the *Risk Management Process* for IT security investments. It aims to give an understanding from which sides the return of an IT security investment comes from, and how it can be valued.

3.1 Definition and Aim

Schechter [84] defines the common term *Security* as follows:

Security: The process of identifying events that have the potential to cause harm (or threat scenarios) and implementing safeguards to reduce or eliminate this potential.

Events in this definition are mostly referred to risk in literature. Risk for Security is defined as:

Risk: is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization [91].

Considering the definition of risks in section 2.2, where Risk was defined "as the combination of the probability of an event and its consequences" [103], the difference between those definitions lies within the narrowed sense of risks, which are related to security. While risk for IT investments can even be used to describe events with a positive outcome, risk within IT security refers to 1) negative effects of events 2) someone/something that is the source of the risk.

Security can be seen as the process of defending an asset against injury or harm. Security also describes the countermeasures implemented by this process [84]. In order to develop an appropriate strategic to prevent events, Threat Scenarios are generated to give a better understanding of the security issues. By developing a general understanding of the events that may lead in a threat scenario, people can better agree on what is at stake and what safeguards reduce the risk.

Threat scenario: A series of events through which a natural or intelligent adversary (or set of adversaries) could use the system in an unauthorized way to cause harm, such as by compromising the confidentiality, integrity, or availability of the system's information [84].

Similar to the definition of security mentioned above, Andrews [6] defines the term *Computer Security* as follows:

Computer security is a discipline, which focuses on techniques, tools, and processes to maintain trustworthy systems in the presence of errors, faults, and intentional misuse

The major difference between those definitions is that the computer security literature divides threat scenarios into three data-centric categories, based on what desired property of the data is lost: confidentiality, integrity, or availability [84], [6], [64]. Schechter [84] describes those basic threat scenarios as follows:

- *Confidentiality*: Information is exposed to someone who should not have access to it.
- *Integrity*: Information is modified in a manner contrary to policy.
- *Availability*: Authorized users are prevented from accessing information or resources in a timely manner.

There are authors who extend those properties by adding further objectives, which can be related to IT security. For example Knorr et al. [62] add *accountability* to those properties. On the other side Soohoo [90] adds authenticity to those objectives. Herrmann et al. [50] define those three properties as a general definition and subsume under security intellectual property, bindings, privacy and anonymity. Those definitions show that security is getting more complex and that there is the need of a general definition on what aspects security is referred.

The definition of Computer Security of Schechter [84] implicates a binary condition of computer security. According to his definition systems can be either secure or insecure. But Computer Security is not a binary Condition. Therefore the definition of Teufel et al. [96] is more suitable for today's view on Computer security:

Security is indicated, if the sum of all individual risks is smaller than the overall risk, which can be accepted [96].

Threat scenarios can become very detailed, when decision makers go deeper into whom, how, and why harm may occur. In order to prevent threat scenarios from happening countermeasures (synonyms: control, security measure, safeguard) are used.

Countermeasure: A policy, process, algorithm, or other measure used to prevent or limit the damage from one or more threat scenarios [84].

Countermeasures prevent or reduce the damage caused by the realization of one or more threat scenarios. When we add a safeguard to a system, we have to consider that this countermeasure may offer additional vulnerabilities. Thus each countermeasure may

lead to the introduction of new, more detailed, threat scenarios that illustrate events in which the countermeasure is penetrated. So, new detailed scenarios may again lead to the definition of new countermeasures.

From the perspective of a business, security is an investment that has to be measured in dollars saved as a result of reduced losses from security breaches. As a result, security modelling often falls under the control of a firm's risk management function [84].

Although IT-Security can be seen as an investment there is still a difference compared to the definition of an IT investment. "Specialists usually make security decisions, but program managers are left wondering whether their investment in security is well spent" [86]. The major difference lies within the Return on Investment. For common IT-Investments we can calculate a benefit for the investment. For example: An organization invests \$10.000 in a new computer system, which increases the productivity of the enterprise about 50%. It is, compared to IT-Security Investments, quite easy to estimate the return of the investment under the current productivity. In contrast IT-Security Investments don't have calculable profit. Security technology benefits depend on how often an attack is expected, how much damage is likely to occur and how effective the security technology is in mitigating the damage from an attack. A lack of information security makes it difficult to quantify what security the organization gets. It is very easy to get a budget for security after a security breach. But investing it in security before makes much more sense [1]. Muhammad [1] proposes the following definition for the *Return on Security Investment*:

The point of maximum return on security investment is where the total cost of security is lowest, including both the cost of security breaches and the cost of the security controls designed to prevent them [1].

According to this definition it is necessary to minimize the costs of preventing threats from happening with minimized costs.

3.2 Planning IT-Security Investments

This section describes a common process to construct a secure system, as it is described in Eckert [36] and in Duncan [34]. Their understanding of planning a secure system can be related to the risk management process for IT. "Risk management is the identification, analysis and treatment of an economic entity's exposures to loss" [27]. The relation of risk management, risk management for IT, and their relation to IT and IT security investments is shown in figure 4. It further shows that risk management is not a one time event. It has to be performed periodically.

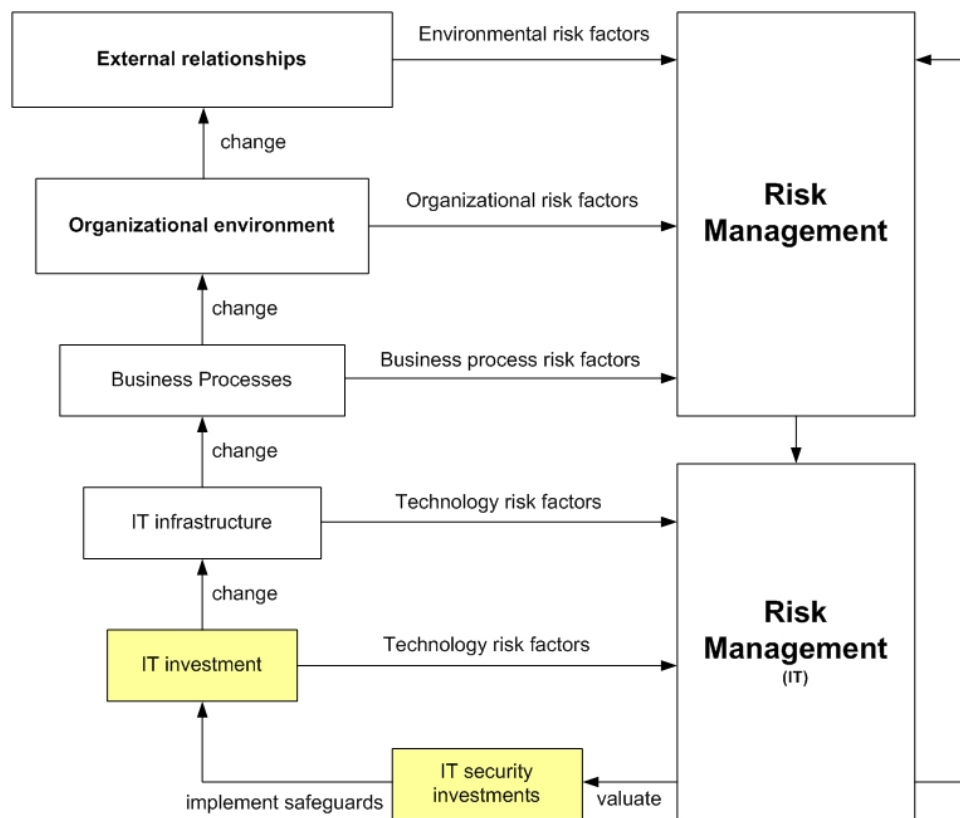


Figure 4: Planning IT security investments

According to Eckert [36] and Duncan [34] the first step is called *Risk Identification*. It consists of determining which risks are likely to affect the project and documenting the characteristics of each risk. There are numerous techniques for risk identification: Checklists, Flowcharting, Interviewing, Brainstorming, . . . [34] The kind of risks differs very much from system to system. Therefore it is quite difficult to formalize all kinds of risks. There are, as mentioned in Eckert [36], groups of risks, where risks can be put in groups like "Attacks from Hackers", "Failures from Employees" or "Technical Failures", . . . which support the security engineer to put the risks in order.

The next step for *IT-Security-Investments* is called *Risk analysis*. It deals with the analysis of possible threats, which can make use of the before evaluated weaknesses and vulnerabilities. To gather these threats a risk tree is may be used, which is very similar

to failure trees in system reliability. When all of these threats are captured, *risk assessment* follows. This is the first step of the risk management process for IT. According to Stonebumer et al [91] it consists of three processes:

- *Risk Assessment*: Risk generation and valuation.
- *Risk Mitigation*: Safeguard generation and valuation.
- *Evaluation and Assessment*: Recurrent evaluation of new risks after safeguard implementation.

In this step the impact of a potential threat and the associated risk for the IT system is valuated. For every risk the probability for the occurrence, the potential damage and the costs to prevent the risk are estimated. An example of a simple risk tree is shown in figure 5. First, the top event risk is defined (In this case: A system crash). Then all risks that can lead to a system crash are analyzed (This example does only cover a very small amount of risks, that can lead to a system crash). The deeper a risk tree is defined, the more accurate are the probability values of the risk. The problem is at this point, that Risk Trees often get too complex with thousands or hundred thousands branches [90].

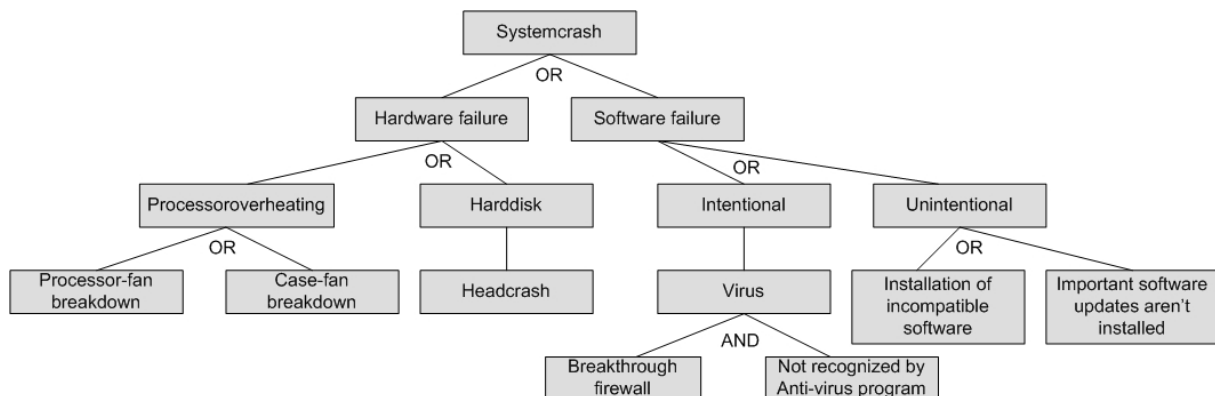


Figure 5: Simple Risk Tree

The security engineer has to decide which risks should be prevented, and which risks should be ignored. But this is not as simple as it seems. A simple thought is: If the cost for prevention of the risk is more than the probability of occurrence multiplied by the possible damage, then measurements to prevent the risk are not necessary. But the real world, especially to deal with risks is not that simple. For example: "What do we do, if a risk has a very low probability of occurrence and very high costs of damage?" This question is discussed in Jablonowski [55], as well as the question "What do we do if probabilities are unknown or irrelevant?" The author of this paper comes to the point, that it is necessary to do a more thorough study of decision methods under conditions where probability information is limited, or of limited value. Bistarelli [14] extended a risk tree by a so called defense tree, which uses in addition attack countermeasures and



Figure 6: Risk Assessment Activities [91]

economic quantitative indexes for computing the defender's return on security investment and the attacker's return on attack.

Stonebumer [91] goes into more detail of the risk assessment process, and defines nine primary steps: System Characterization, Threat Identification, Vulnerability Identification, Control Analysis, Likelihood Determination, Impact Analysis, Risk Determination, Control Recommendations and Results Documentation. Those processes with their specific Inputs and Outputs are shown in figure 6 (cf. Stonebumer [91] for further details). This figure illustrates the basic process for the risk assessment process.

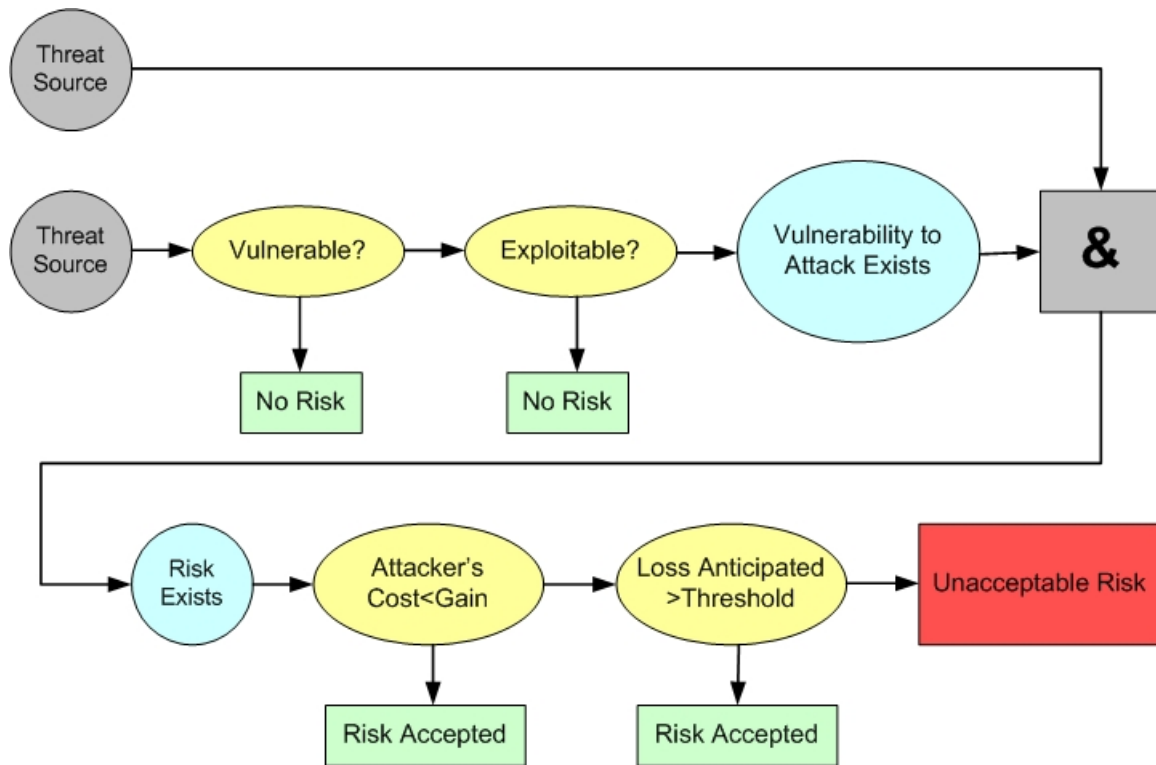


Figure 7: Risk Mitigation Chart [91]

The second step in the risk management process is called: *Risk Mitigation*. This process involves prioritizing, evaluating, and implementing the appropriate safeguards suggested from the risk assessment process. It generates answers to questions like "When and under what circumstances should I take action?", "When should I implement these controls to mitigate the risk to protect our organization?" These questions are addressed by valuation methods. They can be distinguished between quantitative methods mentioned in Schechter [84], Soohoo [90] and Strauss [92], and qualitative methods mentioned in Bundesamt Sicherheit [105], Department of Defense [107] and Common Criteria [106]. According to Gen [65] qualitative methods require human experts in all phases during assessment, including estimating the threat probability, evaluating the asset value, and the vulnerability. This focus on human experts in qualitative methods makes it difficult to automate the risk assessment step. On the other hand quantitative methods calculate risks with mathematical models which are derived from long-term population data. The Risk mitigation chart in figure 7 illustrates this process [91].

Due to the reason that the elimination of all risk is usually impractical or nearly impossible, it is the "responsibility of the senior management, functional and business managers to use the least-cost approach and implement the most appropriate controls to decrease mission risk to an acceptable level." [91], which is one of the major challenges in IT security investments.

The third phase of the risk management process is called *Evaluation and Assessment*,

which is performed periodically. After a system is installed there will usually be changes, updates, software application changes, security policy changes, These changes imply that there will always be new risks depending on the changes that effect the system. Due to this reason it is essential to cycle through the risk management process in order to provide a proper alignment of security strategies.

3.3 Valuation of IT-(Security) Investments

In order to value IT security investments a lot of methods exist. There are a lot of approaches and no satisfying categories in which they can be put in. As mentioned before valuation methods can be divided in qualitative and quantitative methods [65]. According to him qualitative methods (e.g. [105], [107] and [106]) require human experts in all of the phases during assessment, including analyzing the threat probability, evaluating the asset value and the vulnerability and estimating the impacts that threats may cause. Quantitative methods (e.g. [84], [90] and [92]) offer mathematical models for calculating risks derived from long-term population data. In addition we have combinations of both (e.g. [14], [86]).

Due to the large number of different approaches to IT security investments, there are other classifications to find. Soohoo [90] for example uses the terms "Models of the first" and "Models of the second" generation. He distinguishes those groups in their view on security. Whereas models of the first generation (Risk Trees, ALE-based techniques [68]) see Security as a binary condition, second generation (Integrated Business Risk-Management Frameworks, Valuation-Driven Methodologies, Scenario Analysis Approaches, and Best Practice) methodologies take not a binary view on Security. According to him security should be described in relative terms, because the binary view results in assuming that all quantities would be precisely known (single point estimates instead of probabilistically weighted or parameterized ranges of values). These models lead to excessive complexity, poor treatment of uncertainty, and data unavailability [90]. Due to this argument it is essential to see a system as more, or less, secure than another system. This leads to the difficulty of specifying how secure a certain system or component is [35].

Soohoo [90] further classifies second generation approaches into Integrated Business Risk-Management Framework, Valuation-Driven Methodologies, Scenario Analysis Approaches, and Best Practice, for which he states that complexity and uncertainty is still unaddressed. *Integrated Business Risk-Management Frameworks* focus on the bottom line of business impact, without capturing details of computer security interaction (examples are: Microsoft, Mitsui, Capital One Financial, Fidelity Management and Research and BOC Gases Australia). *Valuation-Driven Methodologies* focus on the asset value leaving the likelihood of the risk definition behind. This ignorance of efficiency measures, frequency of security breaches and safeguard costs results in over- or underspending, which

are both economically inefficient. *Scenario Analysis Approaches* develop different scenarios by which computer security is compromised. They have a limited scope on risks and their effects, which lead to simplification, like Valuation-Driven Methodologies, of the assessment process. But they are good to sell security. *Best Practice Approaches* describe policies and safeguards which are implemented in a majority of organizations, which have "proven" to be good. For example Anti virus software for Home PCs are used by most users. There is no need to take extensive evaluation to know that investing in an anti-virus software is sense full for a home PC. This is of course the least analysis-intensive approach, but again it simplifies reality.

Neubauer et al. [75] distinguish between those methodologies in more detail. They differentiate between models focusing on the application of the decision making ([53], [41], [2]) process and methodologies focusing on selecting (portfolios of) security safeguards ([75], [92], [86]).

3.4 Why measuring Security-Investments is hard

The first challenge stems from the definition of security. Although many researchers agree that security is not a binary condition (e.g. [75], [96], [90], [51]) there are still definitions to find (e.g.[84]) that implicates a binary condition of security. SooHoo [90] criticizes such methodologies, because they lead to deterministic models which assume that all quantities would be known.

Accepting the fact that security is not a binary condition results in many challenges. The decision maker has to ask himself "With what level of risk can I live with?". In order to answer this question it is necessary to see security in the context of the organizations strategic drivers. On this way it is necessary to start by defining the objectives of the IT security investment. Although researchers agree that Security is commonly referred to CIA (Confidentiality, Integrity, Availability) (e.g. [84], [6], [64]), there are additional objectives for IT security investments to find (e.g. [62], [90], [52]). So the first challenge starts by defining objectives of the IT security investment which depend on the particular environment where a security strategy should be established.

The next challenge results in valuating those objectives. Therefore it is recommended to see the IT security investment in the organization's strategy. For example the objective *Confidentiality* will be more important for an organization from the health care sector than for a video library. In addition Herrmann [50] proposes to see IT security investment from different perspectives. For this purpose the author defines the informational perspective, functional perspective, dynamic perspective and organizational perspective. Many Researchers agree (e.g. [50], [96], [75], [62], [21]) that an IT security investment has to be evaluated within the business processes and considering strategic drivers of an organization.

3.4.1 Infinite Number of Things that can go wrong

A complete list of the things that can go wrong is impossible to create ... in some cases people have created encyclopedic volumes [20].

There are a number of threats, which make use of weaknesses and vulnerabilities of IT-systems. These can be "Act of God" threats like fire, stroke of lightning, flood, or negligence, or threats like mistakes from users/employees, or technical breakdowns, or threats like system failures, or threats on purpose like hacking, data manipulation, or at least lack of organization like unauthorized access. There are numerous and very different threats to IT-systems, which must be handled technically and organizationally [36]. This challenge lies in the amount of events that can go wrong in an IT system. This number has increased over the past years due to the Internet. Caralli [21] puts it in the following way "These networks are constantly changing and evolving, increasing the organization's exposure (but also its potential for growth)."

For example Buzzard [20] evaluated seven groups of major threats: Intrusion techniques like Social engineering, Monitoring communications, Brute force attacks, Software flaws, configuration errors and malicious software. He evaluated common services (Formal evaluation, Penetration testing, BS7799, EDP auditing and Intrusion detection) which test if an IT systems are protected against those risks. He states that those services test an IT system in isolation although an IT system integrates many different hardware and software. This aspect leads often to overspending in this field where "never has been so much spent, by so many, for so little" [20].

3.4.2 Many Alternatives

... security managers have to decide among too many alternatives [14].

Considering the complexity of an IT system and the amount of things that can go wrong (see Section 3.4.1), there are nearly as much safeguards that reduce the probability of occurrence of risks, as there are things that can go wrong. Therefore determining the acceptable risk level and selecting appropriate safeguards is challenging [14]. According to Butler [86] comparing security designs is challenging because "the strength of the design depends on a relaxed adherence to security engineering design principles". Designs that have a risk mitigation to each risk are usually preferred to those that leave gaps for rarely expected attacks.

3.4.3 Lack of Information

Challenges facing IT security investments are not unique, like in Financial Markets, the insurance industry and others have dealt with risks, lack of adequate statistics, and technological changes [90].

According to the Accounting and Information Management Division [42] "Reliably assessing information security risks can be more difficult than assessing other types of risks, because the data on the likelihood and costs associated with information security risk factors are often more limited and because risk factors are constantly changing" They term the following reasons:

- data are limited on risk factors, such as the probability of a sophisticated hacker attack and the costs of damage, loss, or disruption caused by events that exploit security weaknesses.
- some costs, such as loss of customer confidence or disclosure of sensitive information are difficult to quantify.
- although the cost of the hardware and software needed to strengthen controls may be known, it is often not possible to precisely estimate the related indirect costs, such as the possible loss of productivity that may result when new controls are implemented.
- even if accurate information would be at hand, it would soon be out of date due to vast changes in technology and factors such as improvements in tools available to would-be intruders.

Due to this lack of reliable data determinations of which information security risks are the most significant and comparisons of which controls are the most cost-effective are often inaccurate. Therefore it is essential that organizations identify and employ methods that efficiently achieve the benefits of risk assessment while avoiding costly attempts to develop apparently precise results that are of uncertain reliability [42].

Even if the decision maker has got good statistics at hand he can hardly use them because projects themselves exhibit certain inherent characteristics which have a significant influence over assessment of risk probability. These are according to Hillson et al. [54]: "Projects are unique", "Non-availability of risk actual", "Unknowable risks", and "Estimation vs. Measurement".

This results in inaccurate risk prioritization, which leads to potential failure to focus on the most significant risks. This in turn could lead to selection of inappropriate responses, with attention being paid to wrongly-prioritized risks. Inappropriate response results in

failure to manage risks effectively, with the possibility of loss of confidence in the risk process [54], and to a potential failure to focus on the most significant risks.

In addition, as organizations are exposed to more complexity and uncertainty, because of the increasing use of technology, keeping security activities and strategic drivers aligned becomes more difficult. In the end, finding the right balance between protecting the organization's core assets and processes and enabling them to do their job becomes a challenge for security management [21].

According to Baer et al. [82] the classical risk analysis, which was discussed in section 3.3 is not sufficient for a analysis of a complex IT system. They argument that classical models from probability theory and statistics produces good solutions for future events/risks that have a low probability of occurrence but a high damage for the asset. But it is nearly impossible to have hard statistics at hand for new projects. Even if there are good statistics for parts of a (complex) IT system, it is not recommendable to develop predications for the whole system, because a system is more than the simple sum of its parts. The decision maker should not assign statistics from a project A to a project B. Only a small amount of new projects are comparable to past projects. In a complex system the amount of possible risks is so high, that it is nearly impossible to describe and calculate all possible future events.

3.4.4 View on risks

Security is a business or organizational problem that must be framed and solved in the context of the organization's strategic drivers [21].

But many organizations perform a technology-centric approach view to security by default, due to industry itself and in the selection of skilled personnel. Therefore they see security as a technical specialty in which they do not connect and align security to the organization's strategic drivers. Possible objectives for the valuation of IT security investments are shown in table 1.

Objectives IT-Investments	Objectives IT-Security Investments
1. Financial performance	Confidentiality
2. Business performance	Integrity
3. Strategic performance	Availability

Table 1: Major Objectives for IT-(Security) Investments

A technology centric approach may result in seeing only Confidentiality, Integrity and Availability as objectives. It is clear that IT security may influences the objectives derived from IT investments which are Financial, Business and Strategic Performance. By altering this view on risks a new challenge arises. Security strategy must be sufficiently dynamic to keep up with the rate of organizational and technical change. On balance,

security management must support the organization's quest to be sensing, flexible, and adaptive to its environment and must be able to make a measurable contribution to the organization. This approach provides both advantages and conflict. On the one hand, this approach ensures that the goals of security management are forged from and aligned with the high-level goals of the organization. On the other hand, the strategic drivers and needs of the organization are often in conflict with the actions required to ensure that assets and processes remain productive [21].

3.4.5 Time Perspective

When thinking about risks the decision maker might ask: "When will the risk occur?" or "When will an attack be prevented?" Especially for the last question I have found no approach during my research that answers this question. But it is important to consider the time perspective for risks, and the time value of money. For example if an organization values a safeguard to secure a confidential source code for a new software, the damage which occurs when a person steals this code strongly depends on if he steals that code before or after the release of the software. Another example which illustrates the importance of the time perspective is, if the organization would know that an attack would be in three years, it could invest in something else for three years, and invest in the safeguard that prevents the attack at exactly the same time the attack occurs.

3.5 Summary

This section showed the problematic nature of defining (return on) security, introduced the risk management process for IT security investments, showed the relation to superior risk management process, and to IT investments, introduced a variety of methodologies defining the return on security investments, and elaborated on the challenges which a decision maker has to face in this field.

For IT security and the according components there are many definitions to find. The discussion about security begins at the problematic of defining the components of IT security, and ends at the valuation of IT security investments. They are valued within the risk management process for IT security investments. In this process scenario based approaches are used to generate scenarios, which may compromise the IT system. The major challenge lies within the estimation of probability values, which serve as basis for the valuation of IT security investments. Soohoo [90] states this problem to the point "A model is only as good as the information put into it". Appropriate statistics are often missing when it comes to estimating risk probabilities, risk mitigation rates of safeguards, . . . Researchers agree, that the estimation of input variables can be improved by aligning the valuation of IT security investments to the organization's objectives.

4 About Risks and Uncertainty: A Lack of Information

In order to value IT and IT security investments, it is necessary to estimate input variables for the valuation methods with limited facts at hand. Therefore probability is often assessed subjectively. What determines such beliefs? How do people assess the probabilities or values of uncertain events? Such questions are discussed in Jablonowski [55] primarily from a mathematical point of view. In contrast, Tversky [102] elaborates on this problem from a psychological point of view.

In short the decision-making process is described as: Any decision that people make is based on our present knowledge about the situation at hand. This knowledge comes partly from their direct experience with the relevant situation or from related experience with similar situations. Our knowledge may be increased by appropriate tests and proper analysis of the results, that is, by experimentation. To some extent our knowledge may be based on conjecture and this will be conditioned by our degree of optimism or pessimism. Thus, knowledge may be obtained in several ways, but in the vast majority of cases, it will not be possible to acquire all the relevant information, so that it is almost never possible to eliminate all elements of uncertainty [109]. This section contrasts the decision making process from a mathematical and psychological point of view. This may result in developing mathematical models, to improve the estimation of input variables for valuation methods.

4.1 How Decisions are made

When it is necessary to assess risks, the decision maker barely ever has statistical proof at hand. Mostly, he makes inferences founded on what he remembers from hearing or observing about the risk at question. Psychological research has found several general inferential rules that people apparently use in such situations. These rules are known as heuristics, and are used to reduce complicated intellectual tasks to simpler ones. Despite the fact that they are applicable in many circumstances, it is also apparent that in others they direct to large and continual biases with grave insinuations for the decision making process in areas that are diverse, such as financial analysis and the management of natural hazards [88].

Many people take their decisions based on beliefs about the likelihood of uncertain events such as the outcome of an election or the guilt of a defendant. These beliefs are usually expressed in statements such as "I think that...", "it is unlikely that..." and so on. Often, beliefs concerning uncertain events are expressed in numerical form as odds or subjective probabilities. The question is how one evaluates the likelihood of an uncertain event or the value of an uncertain quantity? According to Tversky [102] people rely

on a restricted figure of heuristic principles that shrink the complex tasks of assessing possibilities and calculating values to simpler judgmental operations which seldom lead to systematic errors. Major heuristics are *Representativeness*, *Availability*, *Adjustment* and *Anchoring*.

4.1.1 Representativeness

The subsequent case shows the mistake naturally made when people try to answer questions such as what the probability that object A belongs to class B is or about what the probability that the event A originates from process B is. Usually, they typically rely on the representativeness heuristic, in which possibilities are assessed by the degree to which A is representative of B [102].

A certain town is served by a larger and a smaller hospital. In the first about 45 babies are born each day, and in the latter about 15 babies, about 50% of all babies being boys. However, the precise percentage varies greatly. Sometimes it may be higher than 50%, and sometimes lower. For a period of 1 year, each hospital recorded the days on which more than 60% of the babies were boys. The results were as follows:

- The larger hospital (21).
- The smaller hospital (21).
- About the same (that is, within 5% of each other) (53).

The values in brackets are the number of students which chose the available answer. Most people judged the likelihood of getting more than 60% boys to be the same for both hospitals. This is apparently because these events are described by the same statistic and are hence likewise representative of the general populace. On the contrary, sampling theory requires that the expected amount of days on which more than 60% of the infants are boys is much greater in the small hospital than the other way round, because a large sample is less probable to stray from 50%. This essential view of statistics is obviously not part of people's range of intuition [102].

Tversky [99] produced a series of events generated by a random process will signify the important characteristics of that source even when the sequence is short. In considering tosses of a coin for heads and tails, for instance, one can observe that the sequence H-T-H-T-T-H is be more likely than the sequence H-H-H-T-T-T, which does not appear par haphazard, and also more probable than the sequence H-H-H-H-H-T-H, which does not embody the fairness of the coin. Accordingly, people expect that the essential characteristics of the process will not only be represented globally in the entire sequence, but also locally in each of its parts, leading to the typical misconception of the Expected Value.

Misinterpretations of chance are not limited to "naive" people. A study of statistical intuitions of qualified research psychologists (e.g. Tversky [102]) discovered a persistent

trust in what may be called the *law of small numbers* according to which even small samples are highly representative of the populations from which they are drawn. The reactions of the examiners mirrored the anticipation that a valid hypothesis about a population will be represented by a statistically considerable outcome in a sample with little esteem for its size. Therefore, the researchers put too much belief in the results of small samples and abhorrently overvalued the repeatability of such consequences. In the actual managing of research, this foregone conclusion leads to the selection of samples of poor size and to over-interpretation of fallouts.

4.1.2 Availability

There are situations in which people assess the probability of an event by the ease with which occurrences they bring to mind. For example, they may assess the risk of heart attack among middle-aged people by recalling such occurrences among one's associates. Similarly, they may evaluate the probability that given business project will fail by imagining various difficulties it could encounter. This judgmental heuristic is called *Availability* [102].

People exercise this heuristic to evaluate an incident as likely or recurrent, if cases of it are easy to picture or call to mind. Often happening events are generally easier to imagine and recall than are infrequent events, and therefore accessibility is often an apposite signal. Nevertheless, availability is also affected by various factors that are not related to frequency of occurrence [88]. For instance, stunning film, like *Jaws* or *The day after tomorrow*, could genuinely alter risk judgments. Availability bias facilitates the explanation of people's misperceptions and flawed decisions as concerns certain natural risks. One crucial inference of the availability heuristic is that discussion of a low-probability hazard may enhance imagination and thus its perceived risk, in spite of what the facts point to [88].

The subsequent paradigm demonstrates this consequence. In a basic demonstration of this effect, people heard a series of renowned personalities of both sexes and were subsequently asked to assess whether the catalogs contained more names of men than women, and to evaluate whether men or women of the list were more famous. In each of the lists, the women were generally more prominent than men. However, the test-subjects mistakenly judged that the class (sex) that had the more famous personalities was the more numerous [100].

4.1.3 Adjustment and Anchoring

In many situations, people start from an initial value that is adjusted to yield the final answer to make estimates. The original value may be the formulation of the problem, or the result of a partial totaling. In any case, adjustments are on the whole inadequate. That is, diverse starting points give way unlike approximations, which are influenced by the initial values. This experience is known as *anchoring* [89].

A study of intuitive numerical estimation illustrates this effect. Two groups of high school students estimated, within 5 seconds, a numerical expression that was written on the blackboard. One group estimated the product $1 * 2 * 3 * 4 * 5 * 6 * 7 * 8$ while the other group estimated the product $8 * 7 * 6 * 5 * 4 * 3 * 2 * 1$. To quickly answer such questions, people may perform a few steps of calculation and estimate the result by extrapolation or modification. For the reason that adjustments are characteristically inadequate, this process should direct to underestimation. Additionally, since the result of the first steps of multiplication is lower in the rising series than in the descending sequence the result of the first sequence should be expected lower than the second. Both estimates were confirmed. The median estimate for the ascending sequence was 512, while the median estimate for the descending sequence was 2250. The correct answer is 40320 [102].

In a study by Bar-Hillel [9] people had to bet on one of three events.

1. *Simple Event*: Draw a red marble from a bag which contains 50% red marbles and 50% white marbles.
2. *Conjunctive Event*: Draw a red marble seven times in succession, with replacement, from a bag which contains 90% red marbles and 10% white marbles.
3. *Disjunctive Event*: Draw a red marble at least once in seven successive tries, with replacement, from a bag containing 10% red marbles and 90% white marbles.

A considerable majority preferred to gamble on the conjunctive event (probability 0.48%) rather than the simple event (probability 0.50%). People also favored the simple event rather than the disjunctive event (probability of 0.52%). Studies of choice, performed by Cohen [26], among gambles and of judgments of probability point out that people tend to overrate the likelihood of conjunctive events and to take too lightly the probability of disjunctive events. These biases are explained as effects of anchoring.

Favoritism in the evaluation of multiple events is principally important in the framework of planning. The thriving achievement of for example the development of a new product usually has a conjunctive nature. In order for the development successful, each of a series of events must take place. Even when each of these actions is very likely, the overall prospect of success can be rather low if there are many events. The general inclination to overestimate the probability of conjunctive events leads to untenable confidence

in the evaluation of the likelihood that a certain plan will do well. In contrast disjunctive structures are encountered in the evaluation of risks. A complex system, such as a nuclear reactor or a human body, will fail if any of its vital components fails. Even if the likelihood of failure in each element is relatively small, the possibility of a general malfunction can be high if many components are involved. Because of this one tends to miscalculate and undervalue the probabilities of failure in complex systems [102].

4.1.4 It won't happen to me

According to Slovic [88] causes of death may be about as good as could be expected, given that they are neither experts in the dangers reflected upon nor showing a representative sample of information. Precise awareness of deceptive samples of information might also be considered to be underlying another evident judgmental predisposition, people's preference to view themselves as so to speak immune to dangers. A considerable majority of individuals think of themselves to drive in a netter way than other average drivers [94], more likely than average to live past 80 [67], less likely than regular to be harmed by products. Although such perceptions are clearly unrealistic, the risks look very small from the perspective of each individual's experience. When, for example, driving a vehicle too fast, tailgating, and the like, poor drivers make trip after trip without an accident. This personal experience gives them the impression of being exceptionally skilled and a feeling of safety. Furthermore, their indirect experience via the news media makes them wrongly perceive that when accidents occur, they happen to others. Given such misleading experiences, people may refuse to take protective actions such as wearing seatbelts [87]. Thus, risks are often underestimated.

4.1.5 Out of sight out of mind

According to Slovic [88] people react to the dangers they perceive. However, if these perceptions are flawed, efforts at private, community, as well as environmental protection tend to be misdirected. For some risks, such as motor vehicle accidents, a wide range of numerical data is readily available. Conversely, for other activities, such as the alcohol and tobacco consumption, risk assessment needs multifaceted epidemiological and experimental studies. Nevertheless, even when there is enough statistical data, the hard facts lead to developing policy. Thus, at some point, human judgment is required to perceive the result as well as to determine their significance [88]. This section puts forth some psychological basics of the risk-assessment process that lead to judgmental boundaries in efficient decision making.

In a study by Fischhoff [39] three groups of college students were asked to estimate the completeness of a fault tree showing the perils linked to ignite a car. While one group saw the full tree, each of the other two received a dissimilar pruned tree. Both trees had

8 categories while the 8th category was called "other", for all other troubles that could occur which were not listed in the other 7 categories. The students were asked to assess the probability of incidence for the 8 categories. This study revealed that the probability judgment of the category "other" was expected higher by those who got a pruned tree. However, the estimates were not that much higher than they should have been.

The designers of a fault trees must make many flexible decisions regarding how to arrange and portray the different sources of hazard. One such judgment that seems to make little dissimilarity is how much detail to put forward. Fischhoff [39] found similar perceptions with varying degrees of detail. Purely mentioning a branch made people estimate exactly how wearisome that branch would look when fully detailed. Still, fusing branches or splitting them made a difference. A given set of problems was judged to account for about 30% more failures when it was presented as two branches that when it was presented as one [88]. This then proves the importance to think about all possible risks that may affect a Computer System. The more risks are missing, the more likely the probability estimates are wrong.

4.2 How Decisions should be made

When confronted with a decision problem, people have to base the decision making process on the amount of information about a future outcome available. For instance if we know for sure that it will rain tomorrow we will bring our raining coat with us. If on the other there is a 30% probability of rain, the "correct" decision, if a rain coat is really necessary, is not as easy. Therefore in decision theory distinguishing between decisions under Certainty, Risk and Uncertainty is crucial. Schniederjans [85] defines them as follows:

- *Certainty*: Under this environment the decision maker knows clearly what the alternatives are to choose from and the payoffs that each choice will bring with certainty if the alternative is chosen
- *Risk*: Under this environment some information on the payoffs are available but are presented in a probabilistic fashion.
- *Uncertainty*: Under this environment no information about the likelihood of states of nature occurring is available. We can only assume that a particular payoff will occur if a given state of nature occurs.

While most decisions are made under Risk and Uncertainty, one still has to decide upon the right methodology depending on the environment in which one selects one of the proper options.

4.2.1 ... under Certainty

Decision theory (DT) is a collection of methodologies and principles employed to make single, alternative choice decisions. The use of DT for IT problems requires assumed mutually exclusive alternatives in the problem situation. One can identify three primary elements in all Decision theory problems [85]:

1. *Alternatives* are the independent decision variables in the DT model. They represent the alternative strategies or choices of action that you select from. When only one choice is allowed, it is called a pure choice problem.
2. *States of Nature* are independent events that are assumed to occur in the future.
3. *Payoffs* are dependent parameters that are assumed to occur given a particular alternative is selected and a particular state of nature occurs

A Decision Theory Model is shown in table 9 and is formulated as follows: Where we can have m alternatives and n states of nature, P_{ij} (where $i=1, 2, \dots, m; j=1, 2, \dots, n$) payoff values are listed by row and column denoting that if a particular alternative is selected and a particular state of nature occurs, the decision making will be rewarded with the specific P_{ij} payoff[85].

Alternatives	States of Nature			
	1	2	...	n
1	P_{11}	P_{12}	...	P_{1n}
2	P_{21}	P_{22}	...	P_{2n}
:	:	:	:	:
m	P_{m1}	P_{m2}	...	P_{mn}

Table 2: DT: Payoff Table [85]

There are two standards for *Certainty* that can be unitized to contribute to the decision making process when the decision maker knows for sure what the payoffs will be in a given state of nature: *maximax* and *maximin*. The maximax criterion works as follows: Select the maximum payoff for each option, and then select the choice with the maximum payoff of the maximum payoffs from step 1. Thus, it is a rather positive criterion, whereas the maximin criterion is a semi-pessimistic advance that assumes the worst state of nature and suggests that one makes the best out of it. It first selects the minimum payoff for each alternative, and then opts for the alternative with the maximum payoff of the minimum payoffs from step 1 [85].

4.2.2 ... under Risk

According to Hanson [48] the leading advance to decision-making under risk is the *expected-utility-theorem*, which is a adaptation of the *expected value* which is as follows:

$$E(x) = w(x_1) * x_1 + w(x_2) * x_2 + \dots + w(x_n * x_n) \quad (2)$$

Where w is the Probability and x_n the consequence or result whereas $x = x(a, s)$ are the actions and s are the states of nature.

For conclusions under risk it is not enough to compute merely the expectancy value, for this does not take into consideration the profits of any given result. A good example which shows exactly this lack is the so called *St. Petersburg Paradox*: Imagine to pay a fixed fee to enter the game. In this game a fair coin will be tossed repeatedly until "tails" first appears, which ends the game. The pot starts an 1\$ and is doubled every time a head appears. You win whatever is in the pot after the game ends. The question is: How much would you be willing to pay for that game? Answering this question using the Expected Value you would calculate:

$$E = 2*0,5 + 2^2*0,5^2 + 2^3*0,5^3 + \dots = \frac{1}{2}*1 + \frac{1}{4}*2 + \frac{1}{8}*4 + \dots = \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \dots = \sum_{k=1}^{\infty} \frac{1}{2} = \infty \quad (3)$$

This sum diverges to infinity. Using the Expected value we would choose to spend as much as possible for this game. In practice however one would not spend more than a few dollars for this game. The precise sum of capital one is prepared to pay depends upon the preferences, on the amount of money available, on the willingness to take risks and so forth. In practice one takes decisions based on the consideration upon the utility which one gets as a consequence of a decision or in this case investment.

Neumann [76] considered this lack and postulated the *Neumann-Morgenstern Expected Utility Theorem* which is formulated as follows:

$$E(u(x)) = \sum_{n=1}^m w(x_n) * u(x_n) \quad (4)$$

Where w is the Probability and x_n the consequence or result whereas $x = x(a, s)$ are the actions and s are the states of nature. Essentially, the Expected value is modified by the $u(x)$ -Utility function. With this function it is possible to assign a weighted average of its utility values under different states of nature to each option.

According to Hansson [48] the argument supporting the expected utility is that this is a rather safe method to make the most of the outcome in the long run. If for instance the expected number of deaths in traffic accidents in a region are 200 per year, if safety belts are compulsory and 300 per year if they are not obligatory, and if these calculations

are correct, approximately 100 more persons per year will actually lose their lives in the latter case than in the former. Hence, when choosing one of these options, it will either lead to fewer or more deaths. If the aim is to reduce the number of traffic casualties, then this can, due to the law of large numbers, be realized by maximizing the expected utility.

The dilemma is that the strength of this argument depends on the large number of accidents that settles random effects in the long run. Therefore, the claim is not applicable on a case-by-case basis with regard to unique or very rare events. Supposing that there is a choice between a probability of .001 of an event that will kill 50 persons and the probability of .1 of an event that will kill one person, random effects will not be leveled out as in the traffic belt case. Hence, it is unclear, when choosing one of the alternatives, whether or not it will lead to fewer casualties than the other option. Then, *ceteri paribus*, there is no convincing reason to maximize expected utility.

Yet, a decision in this case to favor the first of the two alternatives with the lower number of expected deaths may as well depend on a sensible application of expected utility; that is to speak if the decision is included in a adequately large group of decisions for which a meta decision has been made to maximize expected utility. For instance, a criterion for the parameter of chemical substances should be one of maximizing expected utility minimizing expected damage. The steady application of this criterion in all the diverse specific regulatory decisions should minimize the downsides and perils of exposure to chemicals. Thus, the larger the group of decisions that are covered by such a rule is, the more efficient leveling-out effect. Hence, the larger the group of decisions, the larger catastrophic consequences can be leveled out. However, there is a practical as well as an absolute limit to this effect. The practical limit refers to decisions that have to be made in controllable pieces since if too many concerns are put together, then the difficulty of information processing may generate losses that overshadow any benefits that might have been expected. Evidently, decisions can be divided into manageable parts in several ways. However, how this is done may have a strong impact on decision results. In this line, the security of workers against emission may be of more concern if it is grouped together with other issues of radiation at question rather than if it is built-in among other issues of work environment [48].

The total limit to the leveling-out effect is that some extreme effects, such as a nuclear war or a major ecological threat to human life, simply cannot be leveled out even in the hypothetical limiting case in which all human decision-making aims at maximizing expected utility. It is suggested that the Pentagon's use of secret utility assignments to accidental nuclear strike and failure to react to a nuclear attack, as a basis for the construction of command and control devices is a good example [78].

The rule of expected utility value should clarify and emphasize the often misinterpreted difference between a good decision and a good outcome. A person bought a used car that the most reputable garage in town told him had at least 100,000 miles left on it before

needing a major repair. It was clearly a good decision that maximized expected value for this decision maker. But two weeks later, the engine blew up! That was a bad outcome. The outcome was so unlikely, however, that it does not reflect in any way on the quality of the decision. In an clearly uncertain world, even the best decision can have a bad result [5].

Bayesinasim offers an alternative for the inference of probabilities that are taken to be frequencies or potential frequencies. In Bayesianism probabilities can be described as solely mental phenomena as it employs the so called subjective probability. This is a degree of confidence that may vary according to the people. Bayesianism is on the whole an Expected utility theory with subjective utilities as well as subjective probabilities and this is generally called Bayesian decision theory [5]. He identifies four basic principles that employ the notion of Bayesianism:

1) The Bayesian subject has a sound set of probabilistic beliefs. By coherence he means here formal coherence or compliance with the mathematical laws of probability. These principles are the identical with those of objective probability, known from the frequencies of events concerning mechanical devices like dice and coins. A simple example of incoherence would be that a Bayesian subject cannot have a subjective probability of 0.5% that it will rain at any given day and a subjective probability of 0.6% that it will either rain or snow at any given day.

2) The Bayesian subject has a complete set of probabilistic beliefs. Hence, he assigns a subjective probability to each proposition and Bayesian subject has a degree of beliefs about everything. Thus, Bayesian decision-making is always decision-making either under certainty or risk, but on no account under uncertainty or ignorance.

3) The Bayesian subject changes his beliefs according to the conditional probabilities when exposed to new evidence. Conditional probabilities are denoted $p(\cdot|\cdot)$, and $p(A|B)$ is the probability that A, given that B is true. $p(A)$ denotes the probability that A, given everything that you know. As an example, let A denote that it rains in Stockholm the day after tomorrow, and let B denote that it rains in Stockholm tomorrow. Then Bayesianism requires that once you get to know that B is true, you revise your previous estimate of $p(A)$ so that it coincides with your previous estimate of $p(A|B)$. It also requires that all your conditional probabilities should conform with the definition:

$$p(A|B) = \frac{p(A\&B)}{p(B)} \quad (5)$$

These probabilities are subjective because they depend on the information available rather than on propensities or frequencies in the material world.

4) Bayesianism holds that the rational subject selects the alternative with the highest probable utility. Subjective Bayesianism however does not stipulate any particular link between subjective probabilities and objective frequencies or between subjective utilities and monetary or other quantifiable standards. According to Harsanyi [49] it is possible as well choose these utilities and probabilities in a completely cognizant and clear way, in order to make fullest possible employment of the conscious rational as well as intellectual resources, and of the best information on hand subjectively about the person in question and objectively about the environment, the world around. Nevertheless, the basic argument of Bayesian theory does not suggest that one should make a conscious effort to maximize the expected utility rather, its stipulations lie in the mathematical theorem conveying the message that if we act in line with a few significant rationality axioms then we shall without doubt maximize the expected utility [48].

Bayesianism is most accepted by statisticians and philosophers rather than by more practically oriented decision scientists because it is less operative than most other forms of expected utility. Theories based on objective utilities and/or probabilities frequently give rise to predictions that can actually be tested and it is far more complicated to determine whether or not Bayesianism is desecrated [48].

In the simplest form of regret theory, regret is measured and described as the disparity in value between the assets essentially received and the highest level of assets generated by other options [11]. According to Loomes [66] regret theory utilizes a two-attribute utility function that features two measures of satisfaction:

- utility of outcomes as in the *Expected Utility Theorem*.
- quantity of regret.

By regret in this case means "the painful sensation of recognizing that 'what is' compares unfavorably with 'what might have been'." [5]. Regret theory can also give details about how same person may gamble (risk prone behavior) and acquire insurance (risk averse behavior). Both behaviors can be explained in terms of regret-avoidance.

The Prospect Theory was introduced by Tversky [101] It explains the results of experiments with decision problems in terms of monetary outcomes and objective probabilities. Nevertheless, its main features are relevant to decision making overall Prospect theory differs from most other theories as it is "unabashedly descriptive" and makes "no normative claims". Another unique characteristic is that it differentiates between two stages in the decision process.

The first phase is the editing phase. The gains and losses of the diverse alternatives are identified, and then defined relative to some neutral point of reference. More often than not, this reference point matches the current asset position; however, it can be influenced

by the formulation of the accessible prospects, as well as by the outlook of the decision maker.

In the second phase, the evaluation phase the options again are evaluated. Evaluation occurs as if the decision maker utilized two scales of which one substitutes the monetary results given in the problem, while the other replaces the objective probabilities.

The first of these lessons is the importance of the editing phase or the framing of a decision problem. Rationality demands on the framing of a decision problem should be attended to much more carefully than what has in general been done. Secondly, the propensity to either disregard or overweight small possibilities has central normative implications and it would be a fallacy to regard overweighting of small probabilities as an indication of irrationality. It is not a priori irrational to consider the sheer fact that a type of event is likely as a relevant factor, irrespectively of the chance that such an event will actually come about. It is suggested that this is because simple possibilities give rise to process utilities. One may, for instance, favor not to live in a society in which events of a particular type are probable. Then any option in which the probabilities of such an event is above zero will be linked with a negative (process) utility which will have to be considered even if no incident of that type actually takes place [5].

4.2.3 ... under Uncertainty

For Decision-making under *uncertainty*, where the decision maker has no information at all on which state of nature will occur, there are five criteria: Laplace, Maximin, Maximax, Hurwicz and Minimax. The *Laplace criterion* is based on the Principle of Insufficient Information. It is assumed that under this principle that since no information is available on any state of nature, each is equally likely to occur. As such, we can assign an equal probability to each state of nature, and then compute an expected value for each alternative. It is performed by the following steps [85]: 1) Attach an equal probability to each state of nature. For example, if we have five states of nature, probability of each state of nature is 20%. If there are two states of nature, the probability of each state of nature is 50%. 2) Calculate an expected value for each alternative as if the "expected value" criterion is used. 3) Select the alternative with the best expected value computed in Step 2.

The minimax criterion is similar to expected opportunity loss criterion in that it is based on avoidance of loss. The decision using this criterion is based on minimizing the expected opportunity loss. It performs the following steps: 1) Determine the opportunity loss values in not making the best decision in each state of nature. This is accomplished by selecting the best payoff under each state of nature and subtracting all the values in that column from that best payoff. The opportunity loss values can be structured into an opportunity loss table represented by the same framework as the DT payoff table. 2) Determine the maximum opportunity loss values for each alternative. 3) Select the alternative with the minimum opportunity loss value determined in Step 2.

The Hurwics criterion is a compromised approach between the maximin and maximax approaches. In using this criterion the decision maker must subjectively weight the degree of optimism they have in the future. The coefficient of optimism is used for this weighting. The coefficient of optimism is on a scale from 0 to 1 and is represented by the Greek letter α . The closer α is to 1, the more optimistic the decision maker is about the future. The coefficient of pessimism is $1 - \alpha$. Both coefficients are used in the computation of the expected payoffs of each alternative. This criterion is calculated as follows: 1) State the value of α 2) Determine the maximum and minimum payoffs for each alternative 3) Multiply the coefficient of optimism (α) times the maximum payoff, multiply the coefficient of pessimism ($1 - \alpha$) times the minimum payoff, and add these values together to derive the expected value for each alternative 4) Select the alternative with the best expected payoff from Step 3.

4.3 Summary

On the one hand this section focused on heuristics and biases when it comes to subjective decision making. According to Tversky [102] a better understanding of these heuristics and of biases could improve judgments and decisions in situations of uncertainty. On the other hand it described basic mathematical models from decision theory. In addition this section described, that it often comes to misinterpretation of the expected value due to the representativeness heuristic. The availability heuristic influences the probability estimation by the occurrences that can be brought to mind. The adjustment and anchoring heuristics can lead to overestimation of the probability of conjunctive events which lead to unwarranted optimism in the evaluation of the likelihood that a project will succeed or completed in time. On the other hand due to anchoring people will tend to underestimate the overall probabilities for failure in complex systems.

On the other hand this section introduced state of the art methodologies from decision theory. It is necessary to differentiate between decisions under certainty (*maximax*, *maximin* Criterion), risk (*Expected Value*, *Expected Utility Value*, *Bayesianism*, *Prospect Theory*), and uncertainty (*Laplace*, *Maximin*, *Maximax*, *Hurwicz*, *Minimax*) when a mathematical model is applied for a decision problem.

Developing mathematical models on basis of heuristics seems to be close to impossible, because they rely on the individual experiences. One possible way to overcome this problem would be to use questionnaires and change the estimated values according to the decision makers answers. This supports the idea of aligning IT and IT security investments to the organizations objectives in order to improve the estimation of input variables, because input values are continually over- or undervalued, when they are assessed subjective.

5 Evaluation of IT-Investment valuation methods

This section evaluates the following valuation methods for IT investments: Cost/Benefit Analysis from IT investments (ROI, NPV, Cost/Benefit), Real Option Valuation (ROV), Analytical Hierarchy Process (AHP), and Multiobjective Decision Support System (MODS) from Neubauer et al. [74], under the following criteria:

- Type: Financial Technique/Operations Management technique.
- Which challenges are addressed?
- How the challenges are solved?
 - Input/Output variables: This criterion evaluates the Input and Output Variables of the methodologies. This will show 1) how the challenges are understood in both fields and 2) if/how methodologies can be used in both fields.
 - Advantages/Disadvantages: This criterion will evaluate the Advantages/Disadvantages of the methodologies, by 1) contrasting researchers opinions and 2) deriving from how challenges are understood and solved.
- Advantages/Disadvantages? (Contrasting researchers opinions)

This evaluation aims to 1) align the valuation methods according to *low*, *medium*, and *high* risk IT investments, 2) build the basis for the connection between IT and IT security investments.

5.1 Cost/Benefit Analysis

Organizations need some way of formal justification to invest in a new IT system. As mentioned before the 2004 CSI/FBI Computer Crime and Security Survey revealed that fifty-five percent use *Return on Investment(ROI)*, twenty-eight percent use *Internal Rate of Return(IRR)*, and twenty-five percent use *Net Present Value(NPV)*. Those metrics belong to the *Cost/Benefit Analysis*. In other words, most organizations perform a Cost/Benefit analysis and ROI, IRR, NPV are tools of it [23]. As the name implicates this analysis compares the Costs with the Benefits of an investment offering mathematical methods, like ROI, to quantify tangible and intangible costs and benefits. The key concept of evaluating an investment is the time value of money. It assumes that money today has a higher value than the same amount receiving next year. According to Muhammad [1] they refer to a systematic series of concepts and theories that explain the role which information and IT play to assist an organization with product and service design, development, manufacture, and delivery.

Return on Investment (ROI): The ROI is calculated as the profit of the investment (or incremental profits) divided by the cost (or incremental costs) of the investment. The result is a ratio, which can be expressed as percentage, when multiplied by 100. If the return from the investment is greater than the opportunity cost of capital then the investment is worth more than it costs and should be taken. For example a technology investment that costs \$90,000 and will return \$120,000 at the end of one year. Let's assume that this investment has similar risk to that of a security in the capital market with a return of 12 percent. ROI or Return is calculated as follows:

$$Return = \frac{profit}{investment_cost} = \frac{120.000 - 90.000}{90.000} = 0,33 = 33,3\% \quad (6)$$

The return on the investment is 33,3% , which is greater than the opportunity cost of capital of 12% and thus the investment in the computer technology should be taken. While the concept of the Return on Investment is simple, obtaining accurate values of the returns and costs is challenging.

Present value (PV) is the value of future cash flows from an investment today.

$$PV = \frac{C_1}{1+r} + \frac{C_2}{(1+r)^2} + \dots + \frac{C_n}{(1+r)^n} \quad (7)$$

Where $C_1 \dots C_n$ are the expected cash flows for n time periods, and r is the *discount rate*. The discount rate, also called the opportunity cost of capital, is the rate that could be earned by investing in securities of comparable risk to that of the investment.

Net Present Value (NPV): The net present value of net benefits is calculated as the present value of benefits minus the present value of costs discounted back to the present. The net present value of net benefits may be calculated as:

$$NPV = \frac{B_0 - C_0}{(1+r)^0} + \frac{B_1 - C_1}{(1+r)^1} + \dots + \frac{B_n - C_n}{(1+r)^n} \quad (8)$$

Where $B_0 \dots B_n$ are the of benefits for n time periods, $C_0 \dots C_n$ are the expected costs for n time periods, and r is the *discount rate*. Net Present Value decision rule: If NPV is greater than zero, then make the investment. If NPV is less than or equal to zero, then do not make the investment.

Similar to the NPV is the benefit/cost ratio: Except of subtracting the present values of benefits with the present value of costs they are divided:

$$Benefit/CostRatio = \frac{\sum_{t=0}^n \frac{B_t}{(1+r)^t}}{\sum_{t=0}^n \frac{C_t}{(1+r)^t}} \quad (9)$$

Where $B_0 \dots B_n$ are the of benefits for n time periods, $C_0 \dots C_n$ are the expected costs for n time periods, and r is the *discount rate*.

The *Internal rate of return (IRR)* is defined as the discount rate that equates the initial

cost outlay with the present value of future cash flows. Alternatively, it may be defined as the discount rate that would make the NPV of an investment equal to zero. IRR is found by using trial and error to determine the rate that makes the NPV equal to zero. The result of the evaluation of Cost/Benefit Analysis is shown in table 3:

Criteria	Cost/Benefit Analysis
Type	Financial Technique
Aim	Time Perspective, Intangible Cost/Returns
Input Variables	Costs, Benefits, Cashflow, time, interest rate
Output Variables	ROI, NPV, IRR, Benefit/Cost Ratio
Advantage	Time value of money considered simple in concept suitable for "low risk investments"
Disadvantage	missing "operating flexibility" [3] missing consideration of uncertainty, [95] Tendency to decide with one criterion (ROI) [74]

Table 3: Evaluation: Cost/Benefit Analysis

Their strength lies in their simple concept, which can give suitable solutions for low risk investments. One of the major challenges lies within estimating the Costs, and Benefits of IT investments. It is assumed for these metrics that Cost and Benefits are known with certainty. In particular they do not consider non-financial performance measures. Although, they can be included if serious a Cost and Benefit estimation was performed in the first place. Even in this case they give a misleading indication, because "intangible costs and returns are downsized to a single value" [74]. According to Tallon [95] "The key problem with these evaluation techniques is their treatment of *uncertainty* and their failure to consider that outside of a decision to reject an investment outright, firms may have an *option* to defer an investment until a later period. Which gets even more important when the organizations faces extreme variations in market demand and product prices [3]. The problem is that the valuation of information technology investments is particularly challenging because it is characterized by long payback periods, uncertainty, and changing business conditions [10]. Cost/Benefit Analysis does not consider uncertainties underlying IT investment decisions, which force project managers to rely on gut instinct when finalizing IT Investment decisions. Many researchers agree on this point (e.g. [59], [12], [24]) and propose *Real Option Valuation* for managing uncertainties in IT investments.

5.1.1 Sensitivity Analysis

According to Schniederjans [85] *Sensitivity analysis* is defined as a means of determining the reliability of the decision generated from a cost/benefit analysis. In cost/benefit analysis having the actual values of every cost and benefit associated with alternative investments would be ideal. There would be no error when these numbers were known for

certain. However, the values of the costs and benefits, especially those intangibles ones, are only estimates of the true value and thus are associated with some amount of error. A Sensitivity Analysis can be used to evaluate the degree of error. There are many variations to perform a sensitivity analysis. A common way is to select costs, benefits, or other parameters in the NPV calculation, which are assumed to have uncertain values, and vary them in order to check their effects. The analysis involves selecting high and low values of a parameter and assesses the effects on NPV. The result is having a NPV associated with the original value, another NPV calculated with the high value, and another with the low value. The degree of diffusion of these NPVs shows how different values of a parameter affect the final NPV and corresponding decision [85]. Performing a Sensitivity Analysis in this way is possible for all methodologies for IT and IT security investments. There is no doubt, that performing a Sensitivity Analysis is vital for every methodology, which is assumed to have uncertain input variables.

5.2 Real Option Valuation

Up to 60 percent of IT investments depend on its market position and aspirations [28].

According to Trigeorgis [97] in an more and more uncertain and dynamic global market flexibility has become essential for firms to successfully take advantage of future investment opportunities, respond effectively to technological, or competitive changes, or limit losses from bad market developments. Real options considers the importance of waiting or staging flexibility, suggesting that managers should either *wait and see* until substantial uncertainty is resolved and the project is more clearly successful. During the waiting or staging period, new information can be discovered that might affect the value of the project. If future developments turn out worse than expected, the firm has implicit insurance protecting it against losses by choosing not to continue with the project.

5.2.1 Uncertainty in the context of Real Options

In a narrow sense, the real options approach is the extension of financial option theory to options on real (non financial) assets. While financial options are detailed in the contract, real options embedded in strategic investments must be identified and specified. The real options approach works because it helps managers with the opportunities they have to plan [4].

Uncertainty used within the context of Real Options is something different than defined in section 4.2. It is the randomness of the external environment. Managers cannot change its level. Uncertainty is an input into the real options analysis. A firm's exposure to uncertainty, the sensitivity of the firm's cash flows and value to a source of uncertainty, is

determined by a number of factors, together with the line of business, the cost structure, and the nature of contracts to obtain inputs and sell outputs. Managers change asset exposure through investment, after they evaluate the external uncertainty. The adverse economic consequence of a firm's exposure is risk.

Amram et al. [4] state that uncertainty creates opportunities. Once the way of thinking explicitly includes uncertainty, the whole decision-making process changes. They say that Managers should welcome, not fear uncertainty. In rethinking strategic investments, managers have to try to examine their markets in terms of the source, trend, and evolution of uncertainty, determine how external events translate into profits and losses, and then react by positioning the investments to the best advantage of uncertainty.

When a future decision depends on the source of uncertainty, managers care about the range of possible outcomes that the uncertain variable might have when the decision date arrives. The key is the link between possible outcomes and time. Over time the amount of possible outcomes increases. The highest and the lowest values are rather unlikely. The real options approach interweaves the effects of time and uncertainty on valuation and decision making, so it naturally focuses on volatility, the range of uncertainty about growth rates.

5.2.2 Modification of the NPV

The Real Option is basically an expanded or strategic NPV criterion, which is able to capture management's flexibility to alter planned investment decisions. According to Trigerorgis[97] Real Options can be seen as the following modification of the classic Net Present Value:

$$NPV_{Expanded} = NPV_{passive} + ROV_{OptionPremium} \quad (10)$$

Where Option Premium = Flexibility value + Strategic value. Based on this expanded criterion, it can be seen that it may now be justified to accept projects with negative passive NPV of expected cash flows, or delay projects with positive NPV until a later time when Expanded NPV can be maximized under uncertainty.

While the NPV calculation does not consider any decisions that could be done in the future, the Real Options approach does exactly that. Those possible "decisions" which can depend on various factors (for example: Market, Pricing, Risks,...) are called Options. While decisions imply the possibility of infinite consequences an option defines two possible directions. Based on Stock Markets: The option to buy/sell or not buy/sell a specific share. It is necessary to simplify Real-life Problems to adopt the Real Options approach. To show this simplification of Real-Life Problems this thesis presents an example which is based on Trigerorgis [97].

This simplification is done by dividing a complex investment/decision problem into

a few basic blocks connected by some basic decision operations. The four basic decision operations commonly encountered are: choice of the best among several mutually exclusive alternatives (OR), the sum of several (parallel) options (AND), taking the probabilistic average (AVG) of follow-on options across some technical outcome scenarios weighted by the corresponding (actual) probabilities, or investing a portion of a budget in a subset of a range of technological options, and a recursive multi-stage option on an option (or *Compound* option). Valuation proceeds in a recurring way following standard backward risk-neutral option valuation. A simple example of combination of standard options and decision operators for a staged power plant construction (with options to abandon or later expand) is shown in figure 8.

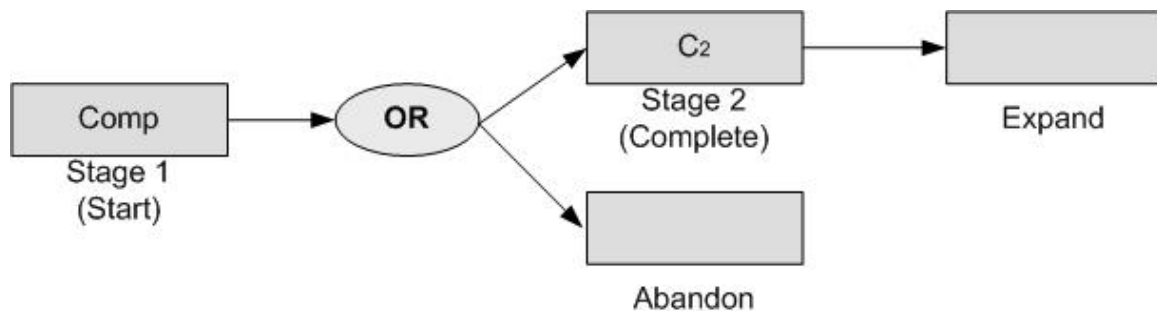


Figure 8: Evaluation: Real Options Approach [97]

5.2.3 Real Option Calculation

Literature refers to two possibilities to calculate an option value. 1) Black Scholes model 2) Binomial Model. The obvious difference between those models is that the value of the option's underlying risky asset follows a lognormal distribution (Black Scholes Model), and a binomial distribution (Binomial Model). Both assume that the value of the underlying asset can increase to infinity, but only fall to zero. The question is which of those models offer a better description of asset's behavior? The answer is, that both models offer the same description over a period of one year, because Benaroch et al. [13] proved that the binomial model converge to those of Black-Scholes model within this time. Therefore the Black Scholes can be used and it is defined as:

$$C = VN(d_1) - Xe^{-r_f T}N(d_2) \quad (11)$$

where

$$d_1 = \frac{\ln \frac{V}{X} + (Tr_f + \frac{\sigma^2 T}{2})}{\sigma \sqrt{T}}, d_2 = d_1 - \sigma \sqrt{T} \quad (12)$$

and C is the value of a call option, $N(\cdot)$ are the probabilities from the cumulative normal distribution (or cumulative standard probability density function), $V_t - X$ indicates the call option's terminal value, $V_t - e^{-r_f T}X$ indicates the call option's current value, V is

the present value of cashflows from investment (risky asset)(or present value of expected project benefits), X extent of follow on investment in IT (exercise price)(or Present value of the expected project costs), T is Time to expiration (length of time that decision can be deferred), r_f is the risk-free rate of return, and σ is the volatility (variance and standard deviation of cash flows) (or variance of expected project returns). Note that for real options a call option is an option to expand.

Criteria	Real Option Valuation
Type	Financial Technique/Operations Technique
Aim	Time Perspective, Intangible Costs/Returns, Lack of Information
Input Variables	Present value of expected cash flows Investment cost Time until opportunity disappears interest rate Project Uncertainty (Volatility)
Output Variables	Option Value/Flexibility Value
Advantage	Time value of money considered suitable for "low/medium risk investments" multiple forms of risk, incomplete information [97] flexibility and increased responsiveness [97]
Disadvantage	Determining input variables is extremely difficult (volatility) [43],[32] high level of mathematics [43],[32] tend to over value project [71] some key assumptions stemming from financial options [25] may be inappropriate for IT investments [95] individual strategic factors are not included missing portfolio selection of real options (interactions)

Table 4: Evaluation: Real Options

According to Garder [43] and Davis [32] determining the input variables for real options is extremely difficult. In addition they emphasize the high level of mathematics, which is too sophisticated for most organizations. One of the key problem of Real Options might be their assumptions deriving from financial options for IT investments [95]: 1) Optimal decision rule for real options(can be project performance indicators) are not always as apparent as for financial options(market price) 2) Financial options assume perfect knowledge of the project value and market replication [25]3) An IT asset acquired through an option can be traded in the open market 4) Exercising the option will not affect the value of the acquired IT asset 5) The variance of the returns (or cash flows) from the IT asset are known 6) Exercising an option is instantaneous.

Some researchers (e.g. [71]) state, that real options lead to overvaluation, because it does not consider implementation time, which has to be executed. This thesis picks up this point in the case study and show that real options can be easily *misused* to overvalue an IT investment. Which could lead to the insight, that the determination of the correct

input variables is vital for a sophisticated real option valuation. Nevertheless Real Options has its advantages, considering flexibility, in their planning and calculation. It stands for no reason that Real Options overcome this lack of basic financial methods (Cost/Benefit) analysis. Whereas further research to make real options more usable, consider interactions between real options (portfolio selection), and include individual strategic drivers, is necessary [95].

5.3 Analytical Hierarchy Process (AHP)

The Analytical Hierarchy Process from Saaty [83] develops factor weights. It utilizes pairwise comparisons to establish factor weights for decision models, produces priorities for a decision choice, and generates accurate statistics to verify its decision analysis. It is a superior decision making methodology because it requires all of the factors in the decision environment to be directly compared with all other factors, providing a more inclusive consideration of the interaction and value of each factor relative to all other factors. It consists of 5 steps [85]:

1) Establish the "decision hierarchy" by determining the overall decision, the factors and the alternatives. In this step the decision maker has to identify the overall decision, the factors that must be weighted or used to make the decision, and the alternative choices from which a decision is to be made. In many cases (notably cost-benefit analysis) it is advantageous to arrange criteria not only within a single hierarchy but to define (at least) two separate hierarchies, one cost hierarchy and a soft facts / benefits hierarchy.

2) Establish the pairwise comparisons of alternatives through a subjective judgment process and using Saaty's nine point scale. In this step the decision maker has to compare each alternative with all other alternatives including one factor at a time. The rating measure scale used for these comparisons forces the decision maker to chose the most desirable alternative and rate the other alternatives on a range from "equally preferred" to the most desirable alternative to "extremely preferred" as it relates to each of the factors. Table 7 illustrates how the alternatives are rated for the factor Security. For example it shows in line 1 that the System B is moderately Preferred ("3") in regard to System A. Or it shows that System C is extremely preferred ("9") relative to System A. Repeat this rating for all other factors. An example of this step is shown in table 5.

Security	System A	System B	System C
System A	1	3	9
System B	$\frac{1}{3}$	1	6
System C	$\frac{1}{9}$	$\frac{1}{6}$	1

Table 5: Evaluation: AHP: Pairwise comparisons of alternatives

3) Compute the factor priorities based on the values from Step 2 as follows: 1) convert values in prior tables to decimals 2) add column totals up 3) divide column totals into

each value in that column 4) sum the resulting row values 5) average the resulting row value.

4) Compute the factor weights based on the same set of procedures from Step as follows: as follows: 1) convert values in prior tables to decimals 2) add column totals up 3) divide column totals into each value in that column 4) sum the resulting row values 5) average the resulting row value.

5) Compute the overall decision priorities. In this step the decision maker uses the factor weights from Step 4 and the values from Step 3 as they were used in the weighted MFSM procedure to compute expected values for the overall decision. The decision will be determined by the calculation of overall decision priority weighting for each of the alternatives. These priorities are used to make the overall decision in the decision hierarchy from Step 1.

6) Determine consistency ratios by first computing a consistency index, and then using the random index values from the Saaty's table. This step includes some additional analysis which permits decision makers to investigate if the subjective ratings are consistent enough to justify using the resulting overall decision priorities. In other words: *AHP checks itself to make sure the ratings consistently make sense for the purposes of using the AHP analysis on which to base a decision.* Therefore it is interesting to describe Step 6 in more detail.

In the first sub-step is necessary to compute the *weighted sum vector* by multiplying the Resulting Priorities from Step 3 by the Original Comparisons from Step 1. The next step results in calculating the Consistency Vector by dividing each of the weighted sum vector values by their related Resulting Priority. After that the consistency index, is calculated as: $CI = \frac{\alpha - n}{n - 1}$ Where CI is the consistency index value, n is the number of items being compared and α is the average of the consistency vector values. The fourth and final sub step involves computing the *consistency ratios* and interpreting it. This ratio is computed by the following formula: $CR = \frac{CI}{RI}$ Where CR is the consistency ratio and RI is a random index value that is obtained from a computed set of tabled statistics. The random index is a statistic designed to identify significant variability of statistical variation in the rating measures.

The interpretation is that for values of $CR > 0.10$ there exists sufficient inconsistency that a re-evaluation of the basic factors and alternatives (that is Step 2, and all the subsequent computations in the remaining steps) should be undertaken. It would show that there is too much inconsistency to use the AHP method and new, more carefully made comparisons are needed before a decision should be made. For values of $CR \leq 0.10$ the decision maker's ratings are relatively consistent and the AHP method can be used for making a decision. Those steps have of course once again be performed for all factors. An example of a result of AHP is shown in figure 9.

The major aim of AHP is to translate strategies into objectives and measures, which

Criteria	Analytical Hierarchy Process (AHP)
Type	Financial/Operations Technique
Aim	Time Perspective, Intangible Costs/Returns, Lack of Information, Multiple Objectives
Input Variables	Criteria (Objectives), Alternatives
Output Variables	"Best Alternative" according to weighted objectives
Advantage	Translation of strategies into objectives and measures Includes financial and non-financial Methods considers relationship among factors Adoptable for various decision making problems (example for security: Bodin [15]) Consistency checking of inputs suitable for medium/high risk investments
Disadvantage	complex (due to pairwise comparison of all factors)

Table 6: Evaluation: Analytical Hierarchy Process (AHP)

is, as section 2.2-2.4 described, essential for valuating an IT investment. Those sections showed that an extensive IT ROI analysis, can affect many aspects of an organization which are often intangible. In addition AHP includes financial and non-financial methods, considers relationship among factors, generates statistics to confirm decision analysis, and supports hierarchical planning through many organizational levels, and the consideration of tangible and intangible benefit categories. The drawback of this method is the high effort of the pairwise comparison of each alternative.

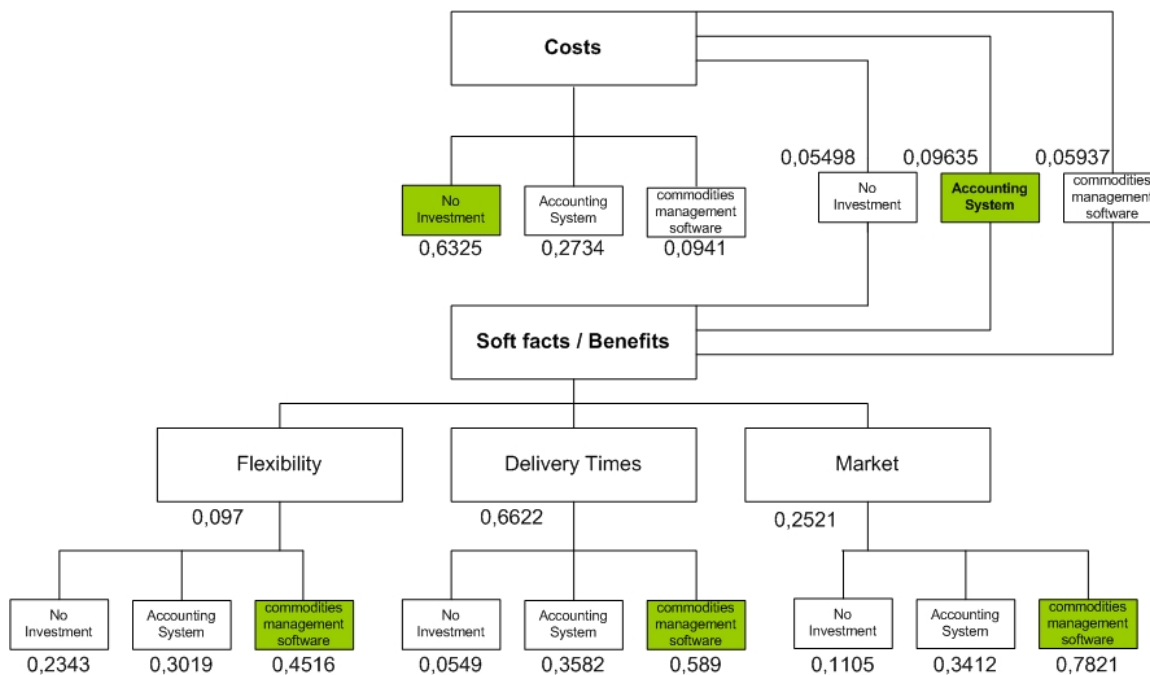


Figure 9: Evaluation: AHP example

5.4 Multiobjective Decision Support for IT investments

The methodologies evaluated in the previous sections did not establish a link to the business process. Neubauer et al. [74] proposes such a methodology, which extends existing business process management (BPM) approaches for evaluating and selecting efficient IT investments. Their methodology focuses on two problems in this field: 1) Using standard software instead of individual IT systems that support the specific business process. 2) The resulting inefficiency with respect to the firm's strategic objectives, by the availability of the core function of the IT system.

According to the authors [74] advantages for an organization with respect to the competitors derived from a IT investment are mainly derived from individual IT system solutions. Their methodology focuses on evaluating such an IT investment. Their methodology aims to support decision makers in identifying the "best" level of IT investment with the extension of an additional phase for valuation, allocation, and selection compared to existing BPM methodologies [74].

In contrast to common Business Process Management Methodologies it provides support for valuating IT investments. The authors implemented such a system as an extension for *Adonis* [56]. With this extension it is possible to import existing BPM models, and to define and valuate existing IT investment alternatives and their dependencies considering different business processes. One of the major challenges lies with a proper design the organization's business processes and the possible IT systems. For this purpose the authors added a so-called *Valuation Level* compared to existing Business Process Management Methodologies. It supports the valuation, allocation and the selection of IT investments considering a given business process, multiple objectives and resource constraints. The major advantage of this phase results in the fact, that the portfolio creation of possible IT investments depends strongly on the organization's strategy. The authors argument, that this approach finds the *ideal* set of IT investments based on a set of business processes, a set of potential IT systems and set of objectives that are related to the corporate strategy. Their methodology consists of four steps:

1) *Criteria Definition*: In this phase the definition of a set of tangible and intangible criteria like functionality, usability and costs takes place.

2) *Data Collection*: In the second step the decision maker has to analyze and rate the IT investment alternatives related to each criterion. Further he has to establish a relation between the business process and the possible IT investment alternatives. The authors propose *Adonis* for this purpose, because it offers to import business process containing the information about costs, the time for executing the business process and eventually existing IT systems that are necessary for the process. The result of this phase is a set of business processes which are mapped to existing or new IT systems.

Generation of IT investment portfolios: For this phase the authors implemented a multiobjective decision support system which determines Pareto-efficient investment alternatives.

Interactive Selection of IT investment portfolios: In this phase the decision maker can finally select the optimal portfolio using an interactive graphical interface that displays the costs and benefits categories. With them the decision maker is able to define lower and upper bounds for the objective values and *playfully* learn about the consequences of his decision.

Criteria	Cost/Benefit Analysis
Type	Operations Technique
Aim(s)	Time Perspective, Intangible Costs/Returns, Lack of Information, Multiple Objectives, Many Alternatives
Input Variables	Set of business processes, Individual benefit criteria, Individual units, Set of IT investment alternatives
Output Variables	"Best Alternative" according to specified preferences
Advantage	Suitable for high risk investments, No intensive a-priori information needed [74], Valuation strongly linked to organization's strategy, (business process, multiple objectives, and resource constraints), Interactive exploration of solution space,
Disadvantage	Too complex for low risk investments

Table 7: Evaluation: Multiobjective Decision Support

This methodology focuses strongly on the challenge *Lack of Information*, by aligning the valuation to the organization's objectives. The major advantage lies in the fact that this methodology strongly focuses on individual software solutions in their valuation. Especially when the existing business process are altered in order to create a competitive advantage the decision maker faces individual software solution, which automate only parts of the business process. This leads to the question "Should I invest in A and/or B", which creates a large amount of alternatives, which have to be valued. At this point it seems, that MODS is the most sophisticated methodology for high risk investments, because it is able to answer this question.

5.5 Summary

This section evaluated Cost/Benefit Analysis from IT investments (ROI, NPV, Cost/Benefit), Real Option Valuation (ROV), Analytical Hierarchy Process (AHP), and Multiobjective Decision Support System (MODS) from Neubauer et al. [74]. Cost/Benefit Analysis is the *state of the art* valuation methodology in this field. Due to the simplicity in concept and calculation it is suitable for low risk investments. But most IT investments depend on risks and uncertainty about future outcomes, which can only be valued through *Sensitivity Analysis* in this methodology. Therefore many researchers propose *Real Option Valuation*, which extends the traditional *NPV* methodology by a flexibility value, which considers risks about future outcomes. The major drawback of this methodology is the challenge of estimating input variables and the high level of mathematics. The Multiobjective Decision Support System overcomes many of those drawbacks by its process based approach. In addition this valuation method considers most challenges, which were shown in section 2. The greatest advantage of this system lies in the consideration of multiple IT investment alternatives, where interactions between them can be considered. Especially, it is possible to value individual software solutions, which automate only parts of the business process, with minimal effort compared to the other valuation methods. For those reasons the presented framework in this thesis will be based on the process based Multiobjective Decision Support System.

Although *AHP* addresses most of the challenges, as well, it is concluded from this evaluation that it should not be used as a *stand alone* methodology. The great advantage of AHP lies within its generality, which makes it possible to adopt it to various situations, because it translates subjective estimates into numbers. This makes it further possible to value different units of measurement. This thesis proposes to use AHP as an *Add on*, which can be used within every of the above described methodologies, in order to support the estimation of input variables, or deciding between IT alternatives, which have similar output values.

Based on this evaluation this thesis proposes to use *Cost Benefit Analysis* for *low*, *Real Option Valuation* for *medium*, and *Multiobjective Decision Support* for *high* risk IT investments. This procedure will be shown in the Case Study in section 7.

6 Evaluation of IT-Security Investment valuation methods

This section evaluates the following valuation methods for IT security investments: Defense trees (including ROSI), Mizzi's [69] Return on Information Security Investments, Security Attribute Evaluation Method, and Multiobjective Decision Support for safeguard selection, under the following criteria:

- Type: Financial Technique/Operations Management technique.
- Which challenges are addressed?
- How the challenges are solved?
 - Input/Output variables: This criterion evaluates the Input and Output Variables of the methodologies. This will show 1) how the challenges are understood in both fields and 2) if/how methodologies can be used in both fields.
 - Advantages/Disadvantages: This criterion will evaluate the Advantages/Disadvantages of the methodologies, by 1) contrasting researchers opinions and 2) deriving from how challenges are understood and solved.
- Advantages/Disadvantages?

6.1 Defense trees for economic evaluation of security investments

The model presented from Bistarelli et al. [14] is a combination of quantitative and qualitative approach. They use financial methods (quantitative approach) comparable to the financial methods evaluated in section 5.1, and combine them with attack trees (qualitative approach) described in section 3.2. In particular they use the following metrics:

- *Single Loss Exposure* (SLE) represents a measure of an organization's loss from a single threat event and can be computed by using the following formula: $SLE = AV * EF$ where, the Asset Value is a synthetic measure of cost of creation, development, support replacement and ownership values of an asset, and the Exposure Factor (EF) represents a measure of the magnitude of loss or impact on the value of an asset arising from a threat event, and is expressed as percentage of the asset value.
- *Annualized Loss Expectancy* (ALE) is the annually expected financial loss of an organization which can be ascribed to a threat and can be computed by using the following formula: $ALE = SLE * ARO$ where the Annualized Rate of Occurrence

(ARO) is a number that represents the estimated number of annual occurrences of a threat.

- *Return on Security Investment (ROSI)* This index is defined as: $ROSI = \frac{(ALE*RM)-CSI}{CSI}$ where RM is the risk mitigated by a countermeasure and represents the effectiveness of a countermeasure in mitigating the risk of loss deriving from exploiting a vulnerability (expressed as a numeric value in $[0,1]$), and CSI is the cost of security investment that an enterprise must sustain for implementing a given countermeasure. If ROSI is a positive number, the cost for the investment is financially justified. Otherwise, if ROSI is zero or a negative number, the investment is not profitable.
- *Return on Attack (ROA)* is the gain that an attacker expects from a successful attack over the losses that he sustains to the adoption of security safeguard S by his target. ROA is defined as: $ROA = \frac{GI}{cost_before_S+loss_caused_by_S}$ where GI is the expected gain from the successful attack on the specified target [29].

An attack tree is an example for a scenario based qualitative analysis. It is an analytical way to describe how attacks against a system can be performed. In order to develop Defensive Trees countermeasures are added to attack trees. An example is shown in figure 10.

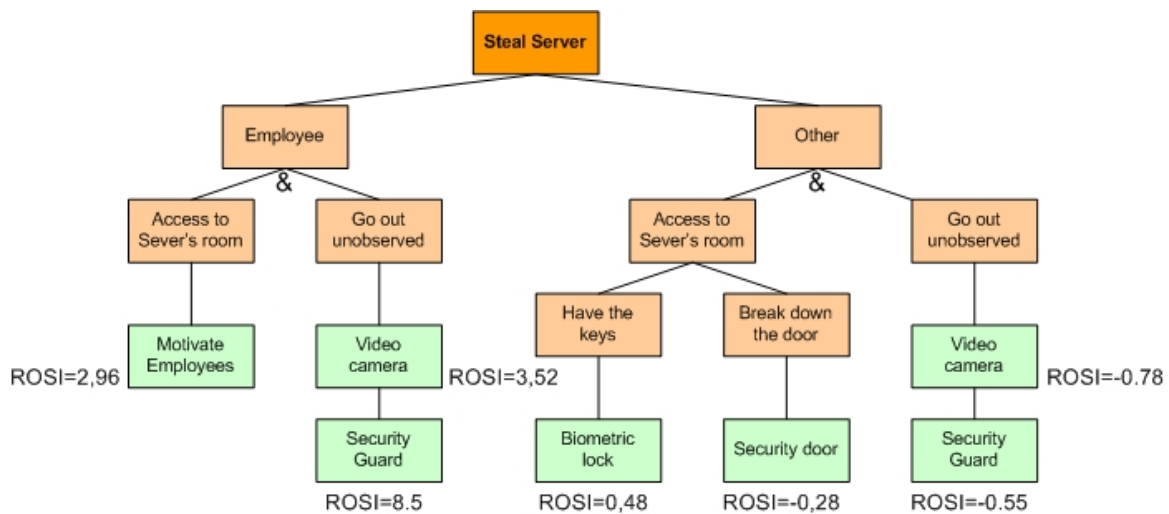


Figure 10: Evaluation: ROSI for "Steal Server" [14]

The following example is shown for the first threat scenario *Steal Server* from figure 15, because it consists of *and-nodes* and *or-nodes*. The difference between these nodes is that the EF and ARO of the and-node has to be considered (since all the leaf vulnerability have to be exploited and not only one). First we have to estimate the *Exposure Factor (EF)* and the *Annualized Rate of Occurrence (ARO)* for each possible Attack in the tree. As mentioned in section 4 it is very important to use correct data for their estimation, which is one major problem in this field. The ARO is estimated with 2 times, which is

expected that an employee would steal the server 2 times/year. The Exposure Factor that an employee steals the server and goes out unobserved is 99%. Note at this point, that in this scenario there are not any countermeasures installed, except a lock to enter the organizations building. The $SLE = AV * EF = 80.000 * 0.99 = 79.200$ and the $ALE = SLE * ARO = 79.200 * 2 = 158.400$. In a similar matter it is possible to calculate that another person gets access to the server's room by having the keys and goes out unobserved or break down the door and goes out unobserved. For this example the ARO is 0.1 (see [14]) and the exposure factor for having the keys is 0.93 and for break down the door 0.90. So the $SLE = AV * EF = 80.000 * 0.93 = 74.400$ and the $ALE = SLE * ARO = 74.400 * 0.1 = 7440$ for "having the keys". The $SLE = AV * EF = 80.000 * 0.90 = 72000$ and the $ALE = SLE * ARO = 72000 * 0.1 = 7200$ for "Break down the door".

In the next step it is necessary to consider the cost of each countermeasure (CSI) and the percentage of Risk Mitigated (RM) in order to calculate the ROI for each countermeasure. The estimation of the CSI and RM are shown in table 12.

With these estimates it is possible to calculate the $ROI = \frac{(ALE * RM) - CSI}{CSI}$ for countermeasure "Motivate Employees" $ROI = \frac{(158.400 * 0.2) - 8000}{8000} = 2,96$, and add them to the defensive tree shown in table 8.

Countermeasure	RM	CSI	ROSI
Motivate Employees	20%	8000\$	2,96
Video camera	10%	3500\$	3,73
Security Guard	90%	15000\$	12,93
Biometric lock	40%	2000\$	0,48
Security door	30%	3000\$	-0,28

Table 8: Evaluation: Return on Security Investments

Table 9 shows the result of the evaluation of defense trees. One of the major disadvantages of this model is the missing consideration of interactions between safeguards. This makes this model impractical. On the other side this model uses sophisticated indexes, which represent *state of the art* methodologies like Cost/Benefit for IT investments. A comparison of those two metrics the ROSI metrics is shown in section 7.2.

Sometimes a countermeasure can mitigate more than one attack/risk. The ROSI can be completely different, because the RM can depend on the specific attack and the ALE can be different depending on the specific attack. Defense Trees lack of the consideration of this aspect.

Criteria	Defense Trees
Type	Quantitative Method/comparable to Financial Method
Aim	Intangible Costs/Returns
Input Variables	Single Loss Expectancy Annual Rate of Occurrence Risk Mitigated Expected Gain from attacker Cost of security safeguard Cost of an attack
Output Variables	Return on Security Investment (ROSI) Annual Loss Expectancy (ALE) Return on Attack (ROA)
Advantage	Combination of qualitative (scenario analysis), and quantitative method (Economic Indexes) Combination of ROSI and ROA [29]
Disadvantage	Lack of empirical data for SLE, and ARO Interactions between safeguards are not considered

Table 9: Evaluation: Defense Trees

6.2 Mizzi's Return on Information Security Investment

The model proposed by Mizzi [69] is based on the calculation of the *Security Expenditure*. The annual security expenditure E_s of an organization is given by

$$E_s = F + B + M \quad (13)$$

Where $F...$ is defined as the annual cost to fix vulnerabilities by the application of system patches or upgrades to the system.

$B...$ is defined as a one time cost to implement defense mechanisms that protect IT assets from possible threats.

$M...$ correlates with B and is defined as annual maintenance cost to cover upgrades and updates of the defense mechanisms.

Mizzi states that there is a probability that an immediate *loss of revenue* followed from a system exploit. Whenever there is a security incident there is a downtime of the system which may be recognized by the IT personnel who interfere. During this system downtime there is the possibility of a loss of revenue. Mizzi [69] shows to components of loss. The first is a function of the Time t that the system was down and the second is the lump sum of money, L_i that is lost immediately. He assumes that the variable loss is a fraction of the value of the information assets at stake, which is quoted annually.

The variable L_t *Total Annual Loss* is defined such that

$$L_t = L_I + \frac{I * t}{365} \quad (14)$$

where, L_i is the instantaneous loss, I is the value of the information assets at stake, t is the time, in days, that the system is unavailable for service. One can also model the loss differently as $A(t)$, availability loss, a function that describes the way that the revenue of the information assets at stake is lost over the time period, t , during which there is an outage. Thus, more generally:

$$L_t = L_I + A(t) \quad (15)$$

Following to the incident and during the time that information is being lost or new revenue can not be made, IT personnel will attempt to repair the system, either by restoring from backups or by replacing equipment, or something else. No matter what method is chosen, there is a financial cost to rebuild R the system which results in the following equation:

$$L_t = L_I + A(t) + R \quad (16)$$

Frequently, the man-hour labor cost r will be the dominant cost, and hence may be rewritten as

$$L_t = L_I + A(t) + r(t) \quad (17)$$

where $r(t)$ is a function describing the annual money spent to rebuilt lost IT assets during the time that the system was down. Normally the length of time (t) during which the system can be expected to be down will depend on the service level agreement (SLA) of the organization. Usually, the lower t is, the more the company will have to pay for the related SLA. Part of the expenditure $r(t)$ can be money that was spent in the SLA.

At this point threats are introduced. Threats relate to the defense mechanisms themselves, like Denial of Service and other attacks on external routers and firewalls that override the defense mechanisms themselves, without necessarily compromising the IT assets, may be attempted. A variable CTB , Annual *Cost to Break*, is defined as

$$CTB = C_D + C_B \quad (18)$$

where C_D is the annual cost to break into the defense mechanisms and C_V is the annual cost to exploit vulnerabilities in the system.

Corresponding *annual damage* D is done to the systems by the attack on both the defense mechanisms D_D and the underlying infrastructure D_i that hosts the information assets and not the information itself. Either way, the damage results in time in which the system has to be repaired. The according cost to repair thus denoted by

$$D = D_D + D_I \quad (19)$$

Mizzi [69] assumes that in our society, a hacker will not manage to break into a system or damage a system unless he spends more than what it costs to build the defense mechanisms. Thus the defense mechanisms should be built such that the cost to break is more than what it costs to build them. Thus for a well designed system:

$$CTB > (F + B + M) \quad (20)$$

Equally, in our society, a hacker is anticipated to be typically set to pay close to, but not more than L_i , if it intends to steal data or possibly $L_i + I(t)$ if it intends to damage an organization's reputation. This will give an indication of the CTB, such that typically there is a motivation to attack the system if

$$CTB < (L_I + A(t)) \quad (21)$$

It is important to add the attacker's reception of information value can be greater than the perception of value of the information owner. In this case the motivation to attack may still be high even with a high CTB. Table 10 compares the indexes presented by Mizzi [69] with ROSI, ALE, ROA, which were evaluated in the previous section.

Mizzi [69]	Bistarelli [14]
1. $L_t = L_I + \frac{I*t}{365}$	$ALE = SLE * ARO$
2. $CTB < (L_I + A(t))$	$ROA = \frac{GI}{cost_before_S+loss_caused_by_S}$
3. $ROSI = \frac{L_t}{3}$	$ROSI = \frac{(ALE*RM)-CSI}{CSI}$

Table 10: Evaluation: Comparison of two quantitative ROSI methodologies

In line 1 Mizzi [69] defines the possible annualized Loss of a threat as *Total Annualized Loss* and Bistarelli [14] defines it as *Annualized Loss Expectancy*. There are two differences:

- The first one is that Mizzi [69] calculates the Total Annualized Loss depending on the time the system is down. Bistarelli [14] does not consider the down time of a system directly. Their calculation is based on the *Single Loss Exposure*, which should include the downtime of a system as loss.
- The second difference is that Bistarelli [14] defines the *Annualized Rate of Occurrence (ARO)* which is theoretically based on statistics. Whereas Mizzi [69] does not use any kind of probability estimates.

The second line lists the *Motivation to Attack* from Mizzi [69] and the *Return on Attack* from Bistarelli [14]. Mizzi [69] calculates the Motivation to Attack based on the gain of the attacker over time, and assumes that if the cost to break are higher than the expected gain, then the attacker would not compromise the system. This is an example for a binary view on security. Instead Bistarelli [14] uses ROA which was introduced and

evaluated from Cremonini [29]. It directly considers the safeguard to prevent an attack for the calculation.

Line 3 shows the return on Investment. Mizzi [69] says quite simple: The money that should be spend on security should not be more than one third of the expected loss.

Criteria	Mizzi's Return on Information Security Investment
Type	Quantitative Method/comparable to Financial Method
Aim	Intangible Costs/Returns
Input Variables	Annual Costs to fix vulnerabilities, one time cost to implement safeguard(s), annual maintenance costs Instantaneous loss, time system is down, value of information asset, costs to rebuild the system, Annual costs to break into system, Annual costs to exploit vulnerabilities, Damage done to the defense mechanisms and infrastructure
Output Variables	Security Expenditure, Total Annual Loss, Annual Costs to Break, Annual Damage, Motivation to Attack
Advantage	Uses many criteria, which may lead to a sophisticated valuation
Disadvantage	The only objective considered is to protect information asset Binary view on security Lack of underlying facts

Table 11: Evaluation: Mizzi's Return on Security Investment

The question which arises from this model is "Why should the organization invest not more than one third of the expected loss?" He refers to one study performed by Gordon [44]. Nevertheless security has to be seen within the organization's strategic drivers. This model is an example for a technology centric approach, because it does not consider any kind of the organization's objectives.

6.3 Security Attribute Evaluation Method

Butler [86] proposes a cost-benefit approach for valuating IT security investments. He uses the Security Attribute Evaluation Method (SAEM) to value IT security investment alternatives. This method starts with the use of a multi-attribute risk assessment, which ends with a weighted list of risks. One of the advantages of SAEM is to prove the security investment consistency. SAEM has four steps:

1) *Risk assessment*: The aim of this step is to identify threats and the consequences of successful attacks. If the organization does not have suitable expectation at hand, Butler [86] proposes a Multi-Attribute Risk Assessment which has four steps:

1. Identification of the outcome attributes (For example: Reputation, Lost Productivity, . . .)
2. Identification of the frequency and outcome attribute values for each threat
3. Ranking of outcome attributes relative to their concerns
4. Generation of threat indexes

When an outcome can have several consequences, these consequences are called *attributes* in the multi-attribute analysis.

After the outcome attributes have been identified, the security engineer has to estimate in the second step the frequency of each threat. For this purpose he can define upper and lower bounds with probability estimates for reaching those bounds. For the third step Butler uses the *Swing Weight Method* to determine relative weights for the outcome attributes. In the fourth step the threat index is calculated which is defined as follows [18]: For each type of attack (a) the threat index (TI) is

$$TI_a = Freq_a * \left(\sum_{i=1}^j w_j * v_j(x_{aj}) \right) \quad (22)$$

where j is the amount of attributes and w_j is the attribute weight and x_{aj} is the "most likely" outcome attribute value for the attack. For considering upper and lower bounds and their related probability Butler [86] modified this equation as follows:

$$\begin{aligned} TI_a = & Freq_a * (p_{low} * \left(\sum_{i=1}^j W_j * v_j(x_{jlow}) \right) \\ & + p_{expected} * \left(\sum_{i=1}^j W_j * V_j(X_{jexpected}) \right) \\ & + p_{high} * \left(\sum_{i=1}^j W_j * V_j(X_{jhigh}) \right)) \end{aligned} \quad (23)$$

The advantage of this calculation lies within the consideration of different value units, so that the relative importance of each type of risk can be captured.

In the second step *Benefit analysis* of the SAEM methodology the effectiveness of a security technology is measured in four steps:

1. Benefit assessment
2. Threat index evaluation
3. Coverage assessment
4. Cost analysis

Butler considers two ways to mitigate a risk: Prevent an attack from occurring or reduce the damage of a successful attack. Therefore IT security technologies are categorized into three categories in the first step of the benefit assessment: Protection, Detection and Recovery. Each Technology has to be at least in one category. These groups show how the risk is mitigated by a particular technology.

In the second step of the benefit assessment phase each security technology is valued by the amount of mitigation for each threat. In the third step, the decision maker faces one of most challenging problems in the Benefit assessment phase: He has to quantify the effectiveness of the safeguards. Often these benefits are estimated subjectively from security specialists, who have experience in the particular technologies. Due to the reason that the effectiveness depends on the organization's ability to employ and maintain the technology those estimates varies across organizations.

In the second step of SAEM the decision maker evaluates, how the benefits affects the Threat index. For this purpose he has to perform an overall assessment because a security technology can reduce the risk from several threats. The result of this phase is the new threat indexes with the percentage change between the old threat indexes and the new ones.

Sometimes the decision about an appropriate IT security investment depends more on the engineering design principles than on the strictly seen effectiveness. Further Butler [86] refers to the *Breadth-of-Coverage* principle, which suggests that there should be at least one mitigation strategy for each risk. For those purposes the third phase of SAEM, *Coverage assessment* has to be performed.

The fourth phase, Selection Criteria Analysis, uses a multi-attribute risk analysis, which focus on valuating nontechnical considerations like maintainability or cultural impact. The aim of this process is to consider implicit attributes that can strongly affect the ability to get expected security benefits in their security designs Butler2002a. As in the first and second step of SAEM this phase uses an additive model to rank each IT security alternative. This phase has three steps [19]:

1. Select Factors
2. Rank Factors
3. Rate Technologies
4. Overall ranking

In the first step we have to determine the most important factors related to the organization's strategy. In this step we can add cost considerations like Maintenance or Purchase Costs [19]. Butler [86] does not elaborate in detail on cost estimation, which can be very time consuming. Instead he proposes to add cost estimates for effective security designs only.

In the second step each selection factor is ranked, based on the importance of each factor, which can be performed through interviews [19]. In the third step the decision maker rates the security technologies by the effectiveness to the particular factors. In the overall ranking phase the additive function $Rank_{security} = \sum w_f * v(security)$ where $v(security)$ is the normalized rank and w_f is the weight for each factor f, is used to calculate the final ranking of the remaining security alternatives.

In addition, but not an integral part of SAEM, Butler [19] [86] proposes the use of a *Sensitivity Analysis*. The author proposes additional interviews or additional research of the estimates to see how this differences change the overall result. *advantages: according to him*

- assumptions are made explicit and they are capturing decision rationale
- the use of a sensitivity analysis shows how assumptions affect design decisions
- design decisions change according to assumption changes
- consistency checking with risk expectations

This methodology overcomes the drawback of Defense Trees, where it could not be considered that one safeguard mitigate more than one attack/risks. It is solved by using the Threat index. Butler uses the *Swing Weight Method*, which is similar to AHP. The advantage of using the Swing Weight Method or AHP is that the risk assessment phase results in relative weights, where different units can be compared in values, which makes it possible to calculate the value of a safeguard, which reduces the ARO of multiple threats. There are two drawbacks of this model: 1) The effectiveness of different measures is expressed in one term (e.g factor weight) 2) The effectiveness of multiple safeguards, which reduce the same vulnerability is not considered.

Criteria	Security Attribute Evaluation Method
Type	Quantitative/Qualitative Method
Aim	Intangible Costs/Returns, Lack of Information, Multiple Objectives,
Input Variables	individual outcome attributes outcome attribute values relative ranking of outcome attributes frequency of attack IT security categories (Protection, Detection, Recovery) Risk Mitigation of IT security alternatives Individual Objectives (here Factors) Safeguard costs
Output Variables	Threat Index Best alternative according to specified criteria
Advantage	qualitative(scenario analysis) & quantitative method(Economic Indexes) Multi-Objective Risk assessment phase different unit values by which the relative importance of each type <i>Sensitivity analysis</i>
Disadvantage	Still challenging: Estimating effectiveness of safeguards

Table 12: Evaluation: Security Attribute Evaluation Method

6.4 Multiobjective Decision Support in IT-Risk Management

Using a Multiojective Decision Support System for IT-Security investments is not a new idea. Strauss et al. [92] have proposed a similar system, which uses complete enumeration. This approach helps IT managers in their attempts a given risk by evaluating and selecting portfolios of security measures. It proposes an attractive portfolio candidates with respect to the decision-maker's preferences. They demonstrated their model by a case study that evaluates the risk of hacking into a Local Area Network (LAN) in an academic environment.

Their model consists of 4 phases: 1) In step 1 a general risk analysis is carried out, the search for security measures commences and alternative security activities are screened. 2) In step 2 the solution space of all feasible and efficient measures are determined. 3) In step 3 a rough selection of portfolios using a quad tree to establish attractive areas is performed. 4) In step 4 a neighborhood search identifies alternatives that may match the decision-maker's preferences even more closely.

It starts by determining the risk factors, by the frequency of successful hacks and the level of damage associated with these hacks. The frequency of a successful first-time hack depends on the complexity of the IT-System. (e.g. number of user accounts, number of super-user accounts, number of workstations, number of servers.). Further they consider the frequency of a hack per user account and super user account which are empirical values.

The damage expensed are assessed by the number of man-hours needed to reconstruct data on a workstation, the number of man-hours needed to reconstruct data on a server, hourly wage for a specialist, hourly wage for a senior specialist, fixed costs per hack on the user level and fixed costs per hack on the super-user level. In their following risk evaluation they follow the principles of a risk-averse behavior, which assumes that damages can only arise as foreseen in the worst case scenario (all data is lost).

Their determination of relevant safeguards (here measures) are performed during a brainstorming session. They define three criteria which are applied to the pool of measures: *effectiveness*: Only those measures that change at least one risk factor is taken into account. *feasibility*: Those measures that cannot be realized due to organizational reasons are excluded. *redundancy*: If one security measure involves isolating the LAN setup from all other networks and a second measure advocates terminating the LAN's access to the Internet, then the latter would be purged from the list of possible measures on the grounds of redundancy, as the other networks at the University also have access to the Internet.

After the measures have been evaluated (i.e., costs and effectiveness have been determined) the best portfolio of measures is selected on the basis of multiple objectives, such as minimizing costs and maximizing both risk reduction and the portfolio's diversification, using the model mentioned above. This has three major advantages:

- The decision-maker has not to provide a-priori information about his preferences by defining upper/lower limits.
- The procedure produces non-dominated portfolios.
- The decision-maker is involved into the solution process and is able to check slightly changed solutions.

The drawback of this model is that phase 2 is based on complete enumeration. Therefore this model can only consider a limited number of security measures. The authors propose the use of metaheuristics such as ACO, GA...

Neubauer et al. [75] refined the multiobjective decision support approach and developed a modified system for security safeguard selection. They propose a workshop procedure called *MOST* (Multi-Objective Safeguard Selection Tool) Their process has two major parts. The first one is an assessment phase which analyzes the current situation and generates safeguard portfolios. The second part reduces those portfolios of safeguards until the *best* one is found. In particular their methodology consists of 6 phases:

1) *Definition of Benefit and Resource Categories*: In this step objectives (here Resource Categories) are defined. Especially the objectives Confidentially, Integrity and Accountability play a major role in an organization's strategy. In a Workshop the decision maker defines the optimal set of security safeguards with regard to the organization's strategy and security policy.

2) *Assets, Vulnerabilities and Threats* In the second step of their workshop assets, vulnerabilities and according threats or sequences of threats have to be identified. This results in the generation of threat scenarios.

3) *Risk Generation and Quantification*: In this step risks are generated by a given threat that can exploit an asset or a group of assets. For each risk the authors assign the *Annual Rate of Occurrence (ARO)*, which represents the probability, that a risk occurs, which is mostly based on statistics.

4) *Safeguards*: In this step safeguards are defined which cost recourses and reduce the *ARO* or reduce the potential damage that can be done by a threat. The authors consider, that risks can be reduced, avoided, transferred or be accepted.

Safeguard Interactions: Some safeguards need to be implemented in combination, which combines their effects on threats. Such interactions are defined in this step.

Portfolio Selection: The performance of this step is supported by a multiobjective decision support system. It calculates the Pareto-optimal portfolio with respect to all other feasible portfolios. The final selection of is supported by an interactive module developed by Stummer and Heidenberger [93].

advantages:

1. defining evaluation criteria according to the corporate strategy
2. assessing and/or refining the existing IT security infrastructure
3. identifying the stakeholders preferences (risks, boundaries)
4. determining the solution space of all efficient safeguard portfolios
5. takes interdependencies between security safeguards into account

The MODS system from Neubauer et al. [75] overcomes the problem of considering a safeguard, which reduces multiple risks by using the Cartesian product of the Vectors:

$$EFF(s, v, b) : S \times V \times B \rightarrow \mathbf{R} \quad (24)$$

where s is the safeguard, v the vulnerabilities reduced, and b is the Benefit Category. The second advantage of MODS is the consideration of Safeguard Interactions. For example: In a firewall should only be invested with a AntiVirus Software. Such dependencies can be applied with the use of Vectors using Portfolio selection. In addition this system

Criteria	Multiobjective Decision Support
Type	Quantitative/Qualitative Method
Aim	Intangible Costs/Returns, Lack of Information, Multiple Objectives, Many Alternatives
Input Variables	Individual Objectives (here: Benefit and Resource Categories) Assets, Vulnerabilities and Threats ARO (frequency) IT security categories (reduce, avoid, transfer, and accept) Safeguard Interactions Risk Mitigation of IT security alternatives Safeguard costs
Output Variables	Best alternative according to specified criteria
Advantage	qualitative (scenario analysis) & quantitative method(Economic Indexes) Multi-Objective decision support Interdependencies between security safeguards
Disadvantage	Still challenging: Estimating effectiveness of safeguards

Table 13: Evaluation: Multiobjective Decision Support

considers the effect of multiple safeguards, which reduce the same vulnerability by using the following formula:

$$\begin{aligned}
 ALE(a, b, \vec{x}) &= VAL(a, b) * \sum_r (EXF(r, b) * ARO(r) * AEFF(\vec{x}, v, b)), \\
 AEFF(\vec{x}, v, b) &= 1 - \prod_i (1 - EFF(s_i, v, b) * x_i)
 \end{aligned} \tag{25}$$

where AEFF is the aggregated effectiveness of all safeguards of the portfolio \vec{x} for vulnerability v and benefit category b .

6.5 Summary

This section evaluated *Defense Trees*, which combine qualitative (attack tree) and quantitative components (Return on Security investments). It compared this quantitative approach, with Mizzi's Return on Security method, and showed the lack of Mizzi's approach, because this method suggests, that for every project one third of the expected loss should be invested into security. Mizzi's approach is a technology centric approach, which does not support to value IT security investments according to the organization's strategic drivers.

Sometimes a countermeasure can mitigate more than one attack/risk. The ROSI can be completely different, because the RM can depend on the specific attack and the ALE can be different depending on the specific attack. Defense Trees lack of the consideration of this aspect. Butler [86] took this lack under consideration, and solved it by using the Threat index. In order to determine the weight Butler uses the *Swing Weight Method*, which is similar to AHP. Therefore this thesis will not go into further detail, of this phase, because AHP has already been discussed in section 5.3 and will be shown in action in section 7.6. The advantage of using the Swing Weight Method or AHP is that the risk assessment phase results in relative weights, where different units can be compared in values, which makes it possible to calculate the value of a safeguard, which reduces the ARO of multiple threats. The drawback of this approach is that the effectiveness of different measures is expressed in one term (e.g factor weight). The MODS system from Neubauer et al. [75] solves this problem by using the Cartesian product of vectors. The second advantage is the consideration of safeguard interactions. For example: In a firewall should only be invested with an AntiVirus Software. Such dependencies can be applied with the use of Vectors using Portfolio selection. The third advantage of MODS is consideration of multiple safeguards, which reduce the same vulnerability.

Due to those reasons MOST will be used to value an IT investment considering the appropriate safeguard selection by extending their definition of risk with the IT investment alternative:

$$R = A \times IT \times V \times T \times \rightarrow \mathbf{R} \quad (26)$$

This extension implies that a security breach only occurs, if a threat exploits a vulnerability, from an IT system, and causes harm to an asset. Each IT alternative may offer different vulnerabilities. For example while a sophisticated implementation of a sql database excludes the vulnerability "bad exception handling", which can be linked to the threat "sql injection", a poor implementation of this database may include this vulnerability.

7 Case Study for IT (security) investments

This section divides itself into two major parts: One case study for low and the other for high risk IT investments. Referring to section 2.3 a low risk IT investments speeds up current business processes, while high risk investments are connected to fundamental changes of the business processes. This differentiation leads to the point, that low risk investments are characterized by complete software solutions, which need slightly adaptations for the specific situation, and high risk IT investments make the development of individual software solutions necessary.

The second part will show how *MOST* can be applied to value different IT investment alternatives, considering the appropriate level of IT security investments.

7.1 The Business Case

The case study for IT investments is performed through automating an accounting process. The business process is shown in figure 11.

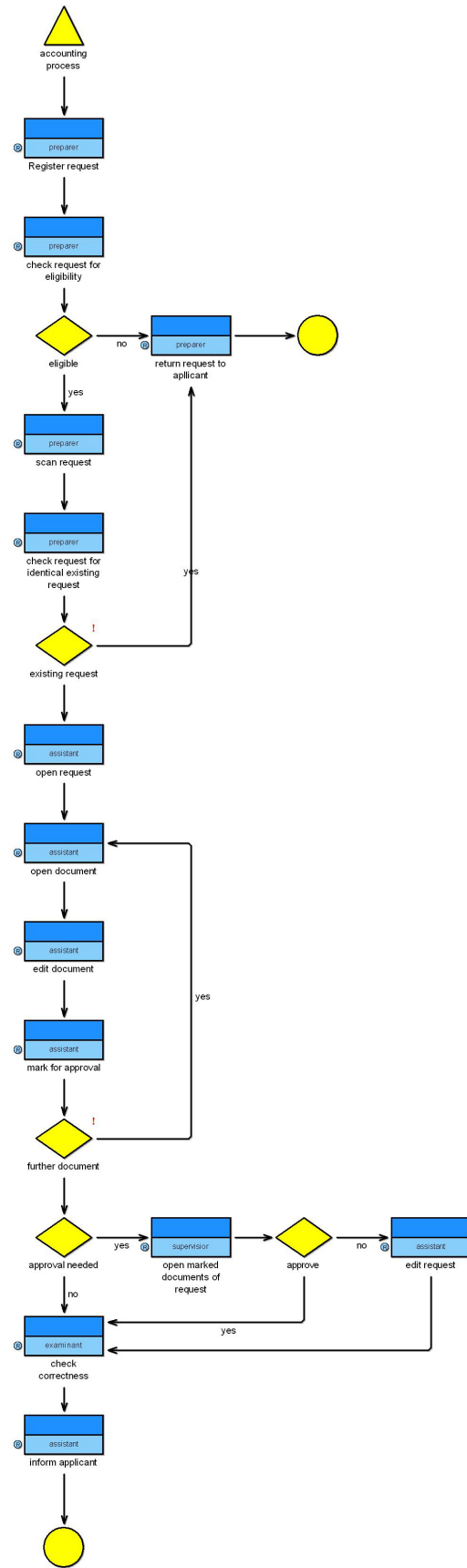


Figure 11: Case Study: Accounting Process

It is the process of a shop, which offers products over their web page. The *state of the art* equation is the *Return on Investment* which is calculated as the profit of the investment divided by the cost of the investment. If the return from the investment is greater than the opportunity cost of capital then the investment is worth more than it costs and should be undertaken. The challenging part for this calculation is to estimate the benefits, and costs of the IT investment. For this purpose it is recommended to use *Adonis*[56], because it effectively supports the estimation of IT investment alternatives.

This shop which presents their commodities over their web page, have a premise, where they have their web-server and their commodities. If a customer wants to buy one of those products he can write an e-mail/mail, call the shop or personally post their order. In any case, the process shown in figure 11 has to be performed, which will be explained shortly.

In the first step the order/request has to be checked for eligibility. An employee has to check if the order/request contains the name, address, phone number of the customer. If so, the employee has to continue by checking if an identical request already exists. If one of these the requests already exist or the name of the customer is not in the order/request, it has to be returned to the customer.

If the request was not returned to the customer, in the next step his request/order will be handed over to the assistant, who is stationed in the warehouse of the shop. He opens the request and checks the order if the ordered product is already stored. If the ordered product is not stored in the warehouse the assistant has to reorder it from the supplier, which is edited in the request. This process is performed as many times as products are ordered. For some products an approval from the supervisor is needed. For example somebody has placed a request for a product above 10000\$. This step finishes with an order status sent to the customer by the assistant.

The shop has sold in the past years most of their products in the shop itself. In the last year the number of orders per mail has increased. Now they get an average of 10 orders a day per e-mail. Therefore they think about investing in a software solution, which automates this process. The efforts of each step of this process are shown in table 14. The *processing time* is the time the activity actually takes from the start to the end. The *waiting time* is the time between the possible start and the actual start of the activity. The probability gives us the value between 0 and 1 with which probability the activity will be performed. The probability value differs from 1 when the activity follows directly a decision.

Those activities are performed by different persons, who get \$20 paid per hour. With the values listed in table 12 *Adonis* calculates with 10000 passes the personnel costs with \$ 1618 per month and \$ 19422 per year.

Activity	Processing time	Waiting Time	Probability
register Request	1 min	30 min	1
check request for eligibility	5 min	0	1
scan Request	45 sec	0	0.9
check request for existing request	6 min	0	1
return request to applicant	3 min	0	0.3
open request	30 sec	10 min	0,8
open document	30 sec	0	1
edit document	7 min	0	1
mark for approval	20 sec	0	1
open marked document for request	2 min	15 min	0.05
edit request	10 sec	2 min	0.01
check correctness	3 min	0	1
inform applicant	2 min	0	1

Table 14: Case Study: Effort of accounting process without IT investment

7.2 IT investment alternatives

Generating a large amount of alternatives of IT systems to automate this process is an easy duty. There are numerous software solutions, which can automate this process. Those alternatives can be divided into 2 categories:

1. Standard/Complete Software Solutions
2. Individual Software Solutions

If an organization reorganizes their business processes in order to achieve a strategic advantage mostly Individual Software Solutions are necessary, because those business processes have *new* requirements to the IT system. In contrast, Standard/Complete Software Solutions can be used if the Organization follows up on automated business processes. As mentioned in section 2.6 this difference can be divided into low and high risk investments. In addition the return of so called low risk IT investments can also strongly depend on market developments. For this reason such IT investments are categorized in medium risk IT investments in this case study, setting aside the fact that individual software solution can even stronger depend on market developments. This part of the case study will show, that there are suitable IT investments methodologies for each of those IT investment categories, while of course the most challenging type is the high risk IT investment.

The reason why this differentiation is necessary is easily explained. If there are three Standard Solutions which all automate this process, then the decision maker has three alternatives when he wants to calculate the ROI of the IT investment. In contrast, if he wants to evaluate individual software solutions he faces a vast larger amount of alternatives or combinations of possible IT systems. For example he gets, an offer A, which automates the components register request, check request, and scan request, an offer B

which automates the components scan request, check request of identical existing request, return request, and open request, and an offer C for open document, edit document, and mark for approval. This leads to the problem that he can not directly compare those alternatives with each other, because they have different functionalities, which may be partly the same. Therefore the question, compared to low risk investment changes from "Should I invest in A or B or C?" to "Should I invest in A and/or B and/or C?" With the last question he faces a *variation* from a mathematical point of view, which concludes that he has n^k alternatives, where n is the amount of elements (in this case it is 2 because we can either take or not take the IT system) and k is the number of alternatives. So in this example he gets 8 alternatives, deriving from 3. Considering 8 alternatives is not that hard, but in the real world decision makers have to consider much more alternatives than those three for a sense full valuation. For example for 20 alternatives he gets 1.048.576, and for 30 we get 1.073.741.824 possible variations. In computer science this is called a NP problem, where the calculation time exponentially increases to the number of alternatives. As the evaluation in section 5 suggests it is close to impossible to calculate such high possibilities with state of the art methods like Cost/Benefit Analysis, Real Option Valuation or AHP. The IT investment alternatives for this case study are shown in table 15.

<i>Low Risk Investment Alternatives</i>					
IT investment	TR	ITR	IC	MC	ITC
CMS 1	19.000	2.000	40.000	3.700	1.200
CMS 2	19.000	5.000	50.000	2.500	1.100
CMS 3	19.000	12.000	64.000	1.300	500
<i>Medium Risk Investment Alternatives</i>					
IT investment	TR	ITR	IC	MC	ITC
DMS 1	9.000	700	18.000	1500	400
DMS 2	10.000	1300	22.000	2200	800
DMS 3	10.000	6000	78.000	2100	1.100
<i>High Risk Investment Alternatives</i>					
IT investment	TR	ITR	IC	MC	ITC
IS 1	3600	690	4600	120	110
IS 2	4100	790	5800	130	110
IS 3	3100	310	4600	100	140
IS 4	3600	840	5700	210	100
IS 5	4400	960	6700	240	120
IS 6	2400	520	5400	280	110
IS 7	3200	560	5700	190	210
IS 8	3600	420	6500	600	180
IS 9	1400	220	6600	600	190
IS 10	2900	350	5900	380	180

Table 15: Case Study: IT investment alternatives

Where TR are the tangible returns, which are derived from Adonis by men hours saved from the automated software, IR are the intangible returns, which are subjectively estimated, IC are the implementation costs, MC are the maintenance costs, and ITC are the intangible costs. At this point it is useful to elaborate in short on the problem of estimating intangible costs and returns. Schniederjans[85] for example proposes four ways to deal with intangible costs/returns: 1) Ignore them, 2) Perform cost/benefit analysis without them but list them and describe their potential effects, 3) Utilize a surrogate measure. A surrogate measure may be the value of a similar benefit or cost that is more easily assigned a value. 4) Perform a survey to determine its value. Considering the first two arguments under consideration, and the intangible Costs/Returns are valued relatively low compared to the tangible Costs and Returns. But this should not lead to the insight the intangible costs and returns are negligible. In fact they may have a strong influence on the project. For example intangible returns in this case study may be: improved customer satisfaction, increased turnover of products, increased employee satisfaction, improved decision making, lower error rates, increased customer loyalty, improved organizational flexibility, better corporate image,...

In addition CMS stands for Complete Management System, DMS stands for Database Management System, and IS stands for Individual System. Those IT investment alternatives automate different parts of the accounting process. Which subprocesses are included by each IT investment alternative are shown in table 16.

IT investment	Included Components
CMS 1 - 3	Complete Atomization
DMS 1	register request - open request
DMS 2,3	open document - inform applicant
IS 1	register request, check request for eligibility
IS 2	scan request
IS 3	check request for identical request
IS 4	return request
IS 5	open request
IS 6	open document
IS 7	edit document
IS 8	mark for approval
IS 9	open marked documents, edit request
IS 10	check correctness, inform applicant

Table 16: Case Study: Included Components by each IT investment alternative

Note that the decision maker may face IT investment alternatives, which have the same functionalities. This can be easily modelled through a functionality categorization like it is presented by Neubauer et al.[74]. This stands especially for individual IT solutions.

7.3 Cost/Benefit Analysis

The *Cost/Benefit Analysis* includes metrics like ROI, NPV, IRR, Cost/Benefit Ratio, . . . but also helps the decision process to consider value-added benefits that are not considered in a simple ROI calculation. According to Schniederjans[85] the Cost/Benefit Analysis starts by defining a problem. This includes a specification of the objectives for an IT investment and a plan to attain those objectives. In this case those objectives are:

- optimize accounting process
- improved costumer service
- step into the e-commerce market

ROI is defined as $ROI = \frac{benefits}{costs}$. With the values from table 15 the ROI for CMS 1 can be calculated as: $ROI = \frac{21.000}{44.900} = 0.468$ which are 46.8%. This simple example shows that although there are clearly more costs than benefits for this IT investment, we still get a ROI of 46.8%. Therefore only ROI solutions over 100% should be taken. In the same manner ROI results with 44.8% for CMS 2, and 47.1 % for CMS 3. Note that this ROI is the value returned in one year. In literature ROI can also have a time perspective. But its time perspective is narrowed, because it does not consider the time value of money. This implies that the investor does nothing with the money instead. This lack overcomes the NPV, which considers the interest rate, which is the return which the investor would get from another investment for sure.

The *Net Present Value* of net benefits is calculated as the present value of benefits minus the present value of costs discounted back to the present. The net present value of net benefits may be calculated as [85]:

$$NPV = \frac{B_0 - C_0}{(1+r)^0} + \frac{B_1 - C_1}{(1+r)^1} + \dots + \frac{B_n - C_n}{(1+r)^n} \quad (27)$$

Where $B_0 \dots B_n$ are the of benefits for n time periods, $C_0 \dots C_n$ are the expected of costs for n time periods, and r is the *discount rate*. For CMS 1 and an interest rate of 10% the PV for Cost and Benefits are calculated as follows:

$$\begin{aligned} PV_{Costs} &= 40000 + 4900 * 1,1^{-1} + 4900 * 1,1^{-2} + 4900 * 1,1^{-3} = 48549 \\ PV_{Benefits} &= 21000 * 1,1^{-1} + 21000 * 1,1^{-2} + 21000 * 1,1^{-2} = 53801 \\ NPV &= PV_{Benefits} - PV_{Costs} = 53801 - 48549 = 5253 \end{aligned} \quad (28)$$

The Decision Rule for the NPV is:

- If NPV is greater than zero, then make the investment.
- If NPV is less than or equal to zero, then do not make the investment.

According to this rule CMS 3 should be taken, with a time perspective of at least three years. Similar to the NPV the benefit/cost ratio is calculated. Except of subtracting the present values of benefits with the present value of costs they are divided [85]:

$$Benefit/CostRatio = \frac{\sum_{t=0}^n \frac{B_t}{(1+r)^t}}{\sum_{t=0}^n \frac{C_t}{(1+r)^t}} \quad (29)$$

Where $B_0 \dots B_n$ are the benefits for n time periods, $C_0 \dots C_n$ are the expected of costs for n time periods, and r is the *discount rate*

The Results of ROI, NPV, and Cost/Benefit ratio are shown in table 17. This table shows, that the ROI calculation can be misleading, because it over values the investment, by not considering the interest rate. This is especially so, when high returns of a project are expected in the future. This is the reason why mostly NPV from Cost/Benefit Analysis is used to value an IT investment.

<i>ROI</i>			
IT investment	1 year	3 years	5 years
CMS 1	46.8%	115.2%	162.8%
CMS 2	44.8%	118.4%	176.5 %
CMS 3	47.1%	134%	212.3%
<i>NPV</i>			
CMS 1	-25363	39	19791
CMS 2	-31455	731	27331
CMS 3	-37454	8617	46692
<i>Benefit/Cost Ratio</i>			
CMS 1	43%	100%	133.8%
CMS 2	41%	101.2%	142.9%
CMS 3	42.9%	112.6%	165.9%

Table 17: Case Study: Cost/Benefit Analysis

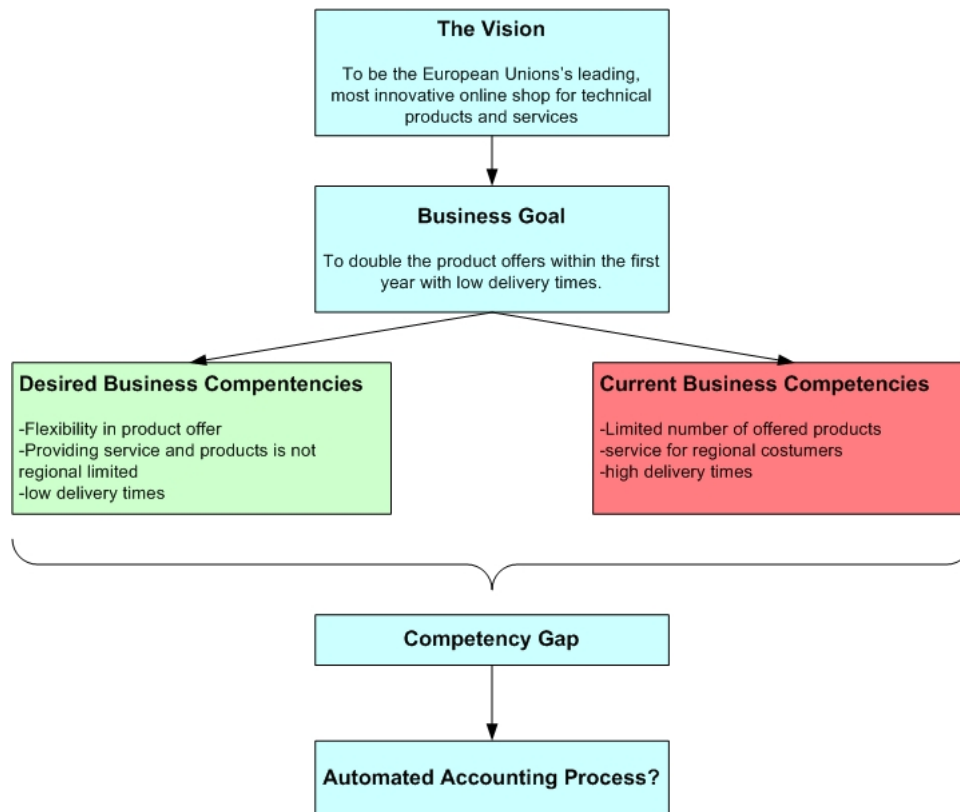


Figure 12: Case Study: Strategic Vision for Real Options

7.4 Real Option Valuation

As shown in the previous section Cost/Benefit analysis lacks of considering a flexibility value, which is necessary, when the IT investment strongly depends on uncertain future outcomes (e.g. Market value). Real Options forces the decision maker to combine a strategic view with uncertainties about future developments in order to judge our IT investment. As shown in section 5.2 the great advantage of Real Options is that it catches the value of flexibility in uncertain future outcomes. From financial option theory an option exists when a decision maker has the right, but not the obligation, to perform an act.

The decision maker has to take a larger vision by seeing the benefits of the IT investment not only in optimizing the accounting process. In this case the IT investment would be the first step into the e-commerce market. Therefore the future cashflow would increase, because the shop would get more costumers due to their new service. The strategic vision of this aspect is shown in figure 12.

The planning phase involves translating the vision into a set of desired business capabilities. In addition, the organization has to decide what operating drivers are needed to support each of the business capabilities. This involves valuating the current operating drivers and determining how to enhance, substitute and build on these drivers to enable the organization to perform the desired business capabilities. For each business capabil-

ity there is an associated value and, similarly, for each of the operating drivers there is typically a related IT investment. The business capability analysis has several important implications for the valuation of IT systems. End business capabilities are secured by making a series of investments, where the go/no-go decision at each stage is contingent on the success of the proceeding stages and the business conditions. The decision maker reacts to changing situations by varying the scope, timing and scale of the investment stages to mitigate downside losses and capture (or even enhance) the upside benefits [63].

Further it is necessary to identify market and project related risks. Project-related risks are determined by how the firm chooses to design, implement and manage the operating drivers. For example, the investment may not pan out as expected because the technology may not deliver on all its promises, or integrating the technology into the organization may be more difficult than foreseen, or there may be cost overruns and time delays. Market related risks, are based on customer acceptance, competitor actions and other factors that affect market demand for the organization's products and services [63]. For simplicity this thesis considers market related risks, because including project related risks in the calculation for Real Options would exceed the scope of this thesis. In this case there are two investment stages:

1. Invest in DMS 1. Time: Beginning
2. Invest in DMS 2. Time: After two years

The first stage is seen in figure 13.

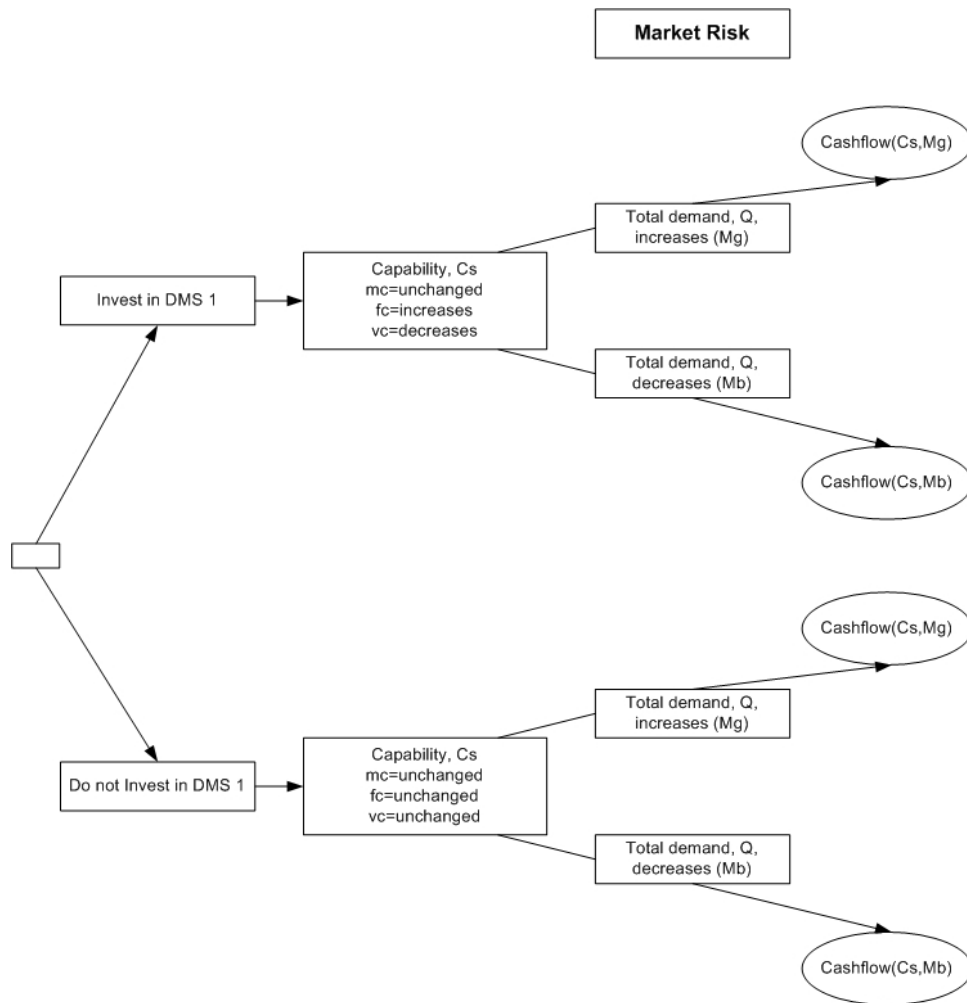


Figure 13: Case Study: First Stage of IT investment

According to Amram et al. [4] the second step consists of *implementing the Option Valuation Model*:

- Establish the inputs: Quite the same as for the discounted cash flow (NPV)
- Value the option with an Option Calculator

The above capability analysis provides the necessary inputs to develop a contingent cashflow. The cashflow modeling structure has to be captured via the three parameters fixed costs, fc , variable costs, vc , and the market share, ms . The Demand for Products of the shop fluctuates. At this time the generated annual revenues of the shop are \$600000. Its fixed costs are 25% fixed costs and 65% variable costs of revenue. As evaluated in the previous section a successful implementation of the accounting system would decrease the variable costs with 5% and increase the fixed costs with 3,3%.

At this point it is necessary to estimate the cashflows for the IT investment. For this purpose it is necessary to model the future demands for the new service and the market development. The demand for online ordering will increase/decrease after the

first investment of the accounting system by 11%. This value comes from the one side of the recordings of the shop itself. The amount of online orderings of the shop increased, considering the past three years, by a mean value of 11%. According to Roland Berger Strategy Consultants the e-commerce market especially for Germany has increased by 73% from 2003 to 2005. But their study shows, that it is very hard for organizations to bind costumers to their organization. So it is quite possible that the costumer demand for ordering online is decreasing although investing in an accounting system. According to the Forrester Research the amount of total internet users will increase with about 66% till the year 2011. About 50% of those are potential costumers for online offers.

The average amount of orders of an online shop are 200 orders per day. Due to this reason investing in the commodities management software is estimated with an increase of the demand of 1000% in three years. This planning is shown in figure 14. This shows that Real Options makes extensive strategic planning necessary.

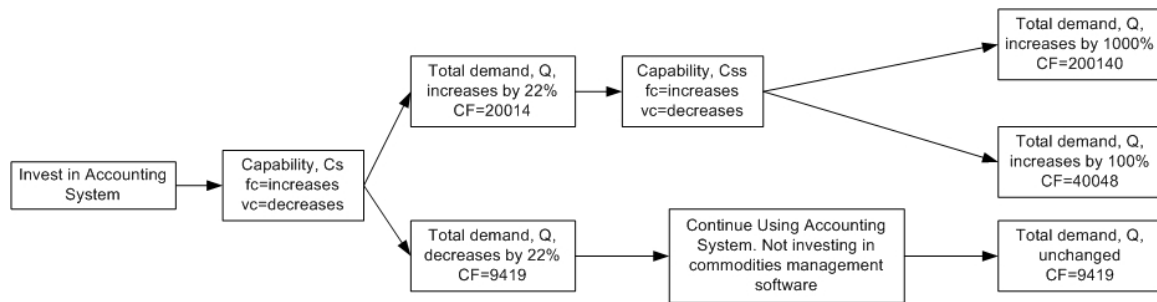


Figure 14: Case Study: Future Cash Flows

7.4.1 Calculating Real Options

$$NPV_{Expanded} = NPV_{passive} + ROV_{OptionPremium} \quad (30)$$

The implementation of a Real Options Calculator is shown in figure 15. This calculator is based on the following formula [37]:

$$C = VN(d_1) - Xe^{-r_f T} N(d_2) \quad (31)$$

where

$$d_1 = \frac{\ln \frac{V}{X} + (Tr_f + \frac{\sigma^2 T}{2})}{\sigma \sqrt{T}}, d_2 = d_1 - \sigma \sqrt{T} \quad (32)$$

C is the value of a call option, $N(\cdot)$ are the probabilities from the cumulative normal distribution (or cumulative standard probability density function), $V_t - X$ indicates the call option's terminal value, $V_t - e^{-r_f T} X$ indicates the call option's current value, V is the present value of cashflows from investment (risky asset) (or present value of expected project benefits), X extent of follow on investment in IT (exercise price) (or Present value of the expected project costs), T is Time to expiration (length of time that decision

can be deferred), r_f is the risk-free rate of return, and σ is the volatility (variance and standard deviation of cash flows) (or variance of expected project returns). Note that this calculator implements a lognormal distribution, as well. For example Kulatika et al.[63] use a lognormal distribution for their Real Option valuation. For the lognormal distribution they estimate D_0 and the time t demand is D_t , then $\ln D_t/D_0$ is normally distributed. In fact there are many variations for Real Option Valuation to find. Elaborating on the different approaches would exceed the scope of this thesis. Therefore this thesis uses the basic Black Scholes model for the Option to expand.

Figure 15: Case Study: Real Options Calculator

Taking the input variables from table 15 for DMS 1 and DMS 2 the IT investment is calculated as follows: $PV = 78635\$$ Note that DMS 1 + DMS 2 added have the same values as CMS 1. The Net Present Value of CMS 1 of Benefits was calculated with $78635\$$ for 5 years. The exercise price for DMS 2 is $22000\$$. With those values and an interest rate of 10% the implementation calculates the values shown in table 18. For DMS 3 the NPV is $94770-90304=4466$.

IT investment	$\sigma = 30\%$			
	1 year	2 years	3 years	4 years
DMS 1 + 2	ROV=58.459	ROV=60.353	ROV=62.066	ROV=63.617
DMS 1 + 3	ROV=24.196	ROV=30.909	ROV=36.986	ROV=42.485

Table 18: Case Study: Real Options Analysis

Taking the Real Option Value of this table for a time to expiration of one year the negative NPV of CMS 1 would get positive. $NPV_{expanded} - 25363 + 58.459 = 33096$.

For DMS 1 + 3 the NPV would still be negative for one year although we get a ROV value of 24.196. This leads to the insight that splitting the IT investment and wait is the more profitable investment. Such results are common, when we compare Real Option Valuation with NPV. For example Kulatilaka [63] presents a case study where they valued an imaging system project with Real Options. They got a value of \$ 2.1 million with Real Options and a negative Value of -380.000\$ with NPV. To see this effect directly you can you can make use of a more sophisticated Real Options Calculator presented by Newton et al. [77].

There are problems of this calculation and the estimated values presented in table 23. First, it is assumed that the values used for this calculation are mean values of possible future paths, like they are presented in the previous section. Second it is assumed, that this return will occur after 5 years of the second investment. If, for example we would take a maximal scope of 5 years, then the $NPV_{expanded}$ would get lower with increasing years to expiration, because direct returns of DMS 2 could not be achieved. Elaborating on this problem and the various modifications of Real Options in order to value an IT investment would go far beyond this thesis.

This section showed the difficulty and effects of the time perspective for IT investments. This effect is similar to the NPV. The higher the time perspective is taken for the returns of the IT investment, the higher the IT investment is valued. This leads to the following problem: IT investments that have low returns at the beginning and high returns at the end may be under valued compared to those which have higher returns at the beginning of the IT investment, although it may be less profitable. The major advantage of Real Options Valuation lies within the strategic plan, performed in the previous section. This shows the complexity of calculating IT investment projects. Note that this was performed for 2 IT investment alternatives only. Even in the more complex case study performed by Kulatilaka [63] for Real Option Valuation only two Investment stages were considered.

7.5 Multi Objective Decision Support

The Multiobjective Decision Support System presented by Neubauer et al. [74] focuses on high risk investment alternatives. Mostly, it is necessary to decide between IT investments which only support a part of the overall functionality needed. This result in one additional problem: The question "Invest in A or B" changes to "Invest in A and/or B", and second in a larger amount of IT investment alternatives. Due to the portfolio based approach it is possible to elaborate on the second question. The individual systems in this table can be added in order to find a solution which is better than CMS 1. Doing so without software support is close to impossible, because in this case there are 2^{10} possible combinations in this simple example. The Graphical User Interface of the implementation of this approach is shown in figure 16.

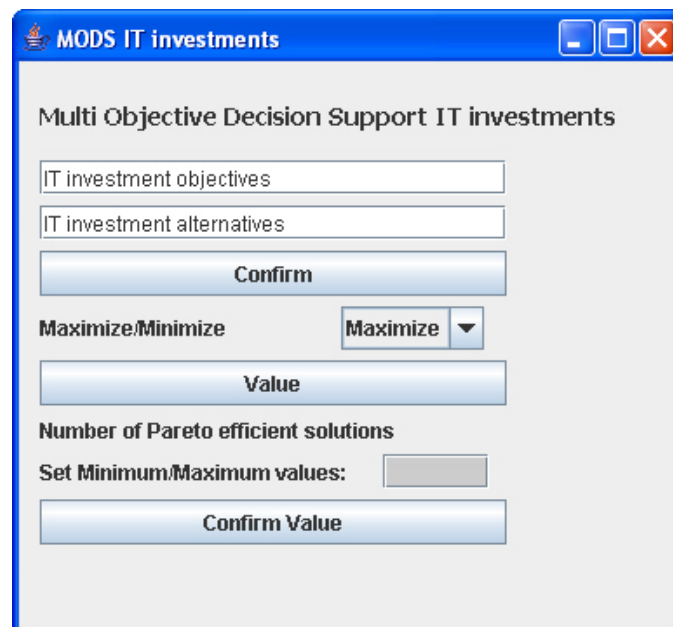


Figure 16: Case Study: MODS Calculator

With this implementation it is possible to define the number and names of objectives, and the values for the IT investment alternatives. Although this implementation can theoretically calculate an unlimited number of objectives and alternatives, it is recommended, not to take more than 20 alternatives to get to a solution within reasonable computation time. For example: For 20 alternatives this implementation needs about 25 minutes to calculate all pareto efficient solutions on a Pentium 4 3.2GHZ HT, because it is based on complete enumeration. This stands for more reasonable optimization algorithms like ARO, NSGA,...

Using the values given in table 15 for IS 1 - IS 10 the algorithm finds 431 pareto efficient solutions. Pareto efficient means that, there is no alternative with higher values in all objectives. In order to find a better solution that DMS 1, the Minimum of 20000 for TR, 2500 for ITR, 38000 for IC, 3700 for MC, and 1200 for ITC was set, which results

in 6 remaining portfolios, represented as a vector $x = (x_1, \dots, x_N)$ where N is number of investment alternatives, shown in table 19.

Vector	TR	ITR	IC	MC	ITC
1 0 1 1 0 0 1 1 1	20000	3170	33000	1590	930
1 1 0 0 1 0 1 1 1	21800	3770	35200	1650	920
1 0 1 0 1 0 1 1 1	20800	3290	34000	1620	950
0 1 1 0 1 0 1 1 1	21300	3390	35200	1630	950
1 0 0 1 1 0 1 1 1	21300	3820	35100	1730	910
1 0 0 0 1 1 1 1 1	20100	3500	34800	1800	930

Table 19: Case Study: MODS IT investments

It is assumed that all alternatives (IS 1 to IS 10) have different functionalities. Often they have same functionalities. This can be easily framed by a functionality objective for each alternative with a percentage value. The NPV values of the portfolio selections are still negative, because the return values were taken for a one year perspective. Therefore a more suitable objective than tangible returns would be for example Cost Reduction. This example shows that for high risk investments a multiobjective decision support approach is necessary to cope with this increasing complexity. At this point there is still the problem which alternative from the remaining six to chose. For this purpose it is possible to use AHP, because it can take intangible criteria under consideration, or in this case value the remaining solutions according to individual preferences with regard to the objectives.

7.6 AHP Analytic Hierarchy Process

The methods in the previous sections assumed, that we have intangible Costs and Benefits in form of costs and returns in \$ values at hand. But what if the resulting values are quite similar to each other, and when it is necessary to compare those alternatives according to the organization objectives? For this purpose it is possible to use AHP, which helps the decision maker to translate subjective estimates into numbers. It utilizes pairwise comparisons to establish factor weights for decision models, establish priorities for a decision choice, and generate accurate statistics to confirm its decision analysis[85]. The pairwise comparison uses values: 1. is Equally preferred, 2. Equally to moderately preferred, 3. Moderately preferred, 4. Moderately to strongly preferred, 5. Strongly preferred, 6. Strongly to very strongly preferred, 7. Very strongly preferred, 8. Very to extremely strongly preferred, 9. Extremely preferred.

The major advantage of AHP lies in the consistency checking. It valuates if the estimates are consistent. It is based on the following assumption: If A is preferred to B ($A > B$, and C is preferred to A $C > A$, then we can assume that $C > B$ (transitive). Is the last estimate valuated this way by the decision maker then the estimation is consistent. A comparison Matrix is defined as consistent if $a_{ij}a_{jk} = a_{ik}$ for all i,j,and k. The Con-

sistency Ratio $CR = \frac{CI}{RI}$ where RI is the Random Consistency Index and $CI = \frac{\lambda_{max} - n}{n-1}$, where λ_{max} is the maximum of eigenvalues of the matrix, and n is the number of alternatives. The Random Consistency Index is derived from randomly generated reciprocal matrices to see if it is about 10% or less. Our decisions are assumed to be consistent when CI is <10% [57].

First it is necessary to value the alternatives according to each objective with each other. The resulting matrices of this subjective estimation is seen below:

$$\begin{aligned}
 \mathbf{TR} &= \begin{pmatrix} 1 & 0.11 & 0.143 & 0.2 & 0.2 & 0.5 \\ 9 & 1 & 4 & 3 & 3 & 8 \\ 7 & 0.25 & 1 & 0.5 & 0.5 & 3 \\ 5 & 0.33 & 2 & 1 & 1 & 4 \\ 5 & 0.33 & 2 & 1 & 1 & 4 \\ 2 & 0.125 & 0.33 & 0.25 & 0.25 & 1 \end{pmatrix}, \mathbf{ITR} = \begin{pmatrix} 1 & 0.143 & 0.33 & 0.25 & 0.11 & 0.2 \\ 7 & 1 & 5 & 4 & 0.5 & 3 \\ 3 & 0.2 & 1 & 0.5 & 0.2 & 0.33 \\ 4 & 0.25 & 2 & 1 & 4 & 0.5 \\ 9 & 0.2 & 5 & 0.25 & 1 & 4 \\ 5 & 0.33 & 3 & 2 & 0.25 & 1 \end{pmatrix} \\
 \mathbf{IC} &= \begin{pmatrix} 1 & 8 & 4 & 5 & 5 & 4 \\ 0.125 & 1 & 0.33 & 1 & 1 & 0.5 \\ 0.25 & 3 & 1 & 4 & 4 & 3 \\ 0.2 & 1 & 0.25 & 1 & 1 & 0.5 \\ 0.2 & 1 & 0.25 & 1 & 1 & 0.5 \\ 0.25 & 2 & 0.33 & 2 & 2 & 1 \end{pmatrix}, \mathbf{MC} = \begin{pmatrix} 1 & 3 & 2 & 2 & 5 & 8 \\ 0.33 & 1 & 0.5 & 0.5 & 4 & 6 \\ 0.5 & 2 & 1 & 1 & 3 & 5 \\ 0.5 & 2 & 1 & 1 & 4 & 6 \\ 0.2 & 0.25 & 0.33 & 0.25 & 1 & 3 \\ 0.125 & 0.166 & 0.2 & 0.167 & 0.33 & 1 \end{pmatrix} \\
 \mathbf{ITC} &= \begin{pmatrix} 1 & 0.5 & 3 & 3 & 0.33 & 1 \\ 2 & 1 & 3 & 3 & 0.5 & 1 \\ 0.33 & 0.33 & 1 & 1 & 0.33 & 0.5 \\ 0.33 & 0.33 & 1 & 1 & 0.33 & 0.5 \\ 3 & 2 & 3 & 3 & 1 & 2 \\ 1 & 1 & 2 & 2 & 0.5 & 1 \end{pmatrix}, \mathbf{Obj} = \begin{pmatrix} 1 & 3 & 2 & 5 & 9 \\ 0.33 & 1 & 0.33 & 4 & 7 \\ 0.5 & 3 & 1 & 5 & 8 \\ 0.2 & 0.25 & 0.2 & 1 & 3 \\ 0.11 & 0.143 & 0.125 & 0.33 & 1 \end{pmatrix}
 \end{aligned}$$

The solution matrix is given by:

$$\mathbf{Solution} = \begin{pmatrix} 0.01328 & 0.17878 & 0.05355 & 0.07367 & 0.07367 & 0.02032 \\ 0.00485 & 0.05109 & 0.01036 & 0.03465 & 0.05252 & 0.02508 \\ 0.14112 & 0.01899 & 0.06911 & 0.02018 & 0.02018 & 0.03523 \\ 0.02480 & 0.01042 & 0.01385 & 0.01494 & 0.00452 & 0.00229 \\ 0.00524 & 0.00678 & 0.00248 & 0.00248 & 0.01034 & 0.00524 \\ 0.06897 & 0.05806 & 0.03518 & 0.04202 & 0.04202 & 0.04878 \end{pmatrix}$$

Adding the columns up from this matrix results in the overall ranking: Port 1 Value = 0.18929598212209015, Alternative= Port 2 Value = 0.2660541567501337, Alternative= Port 3 Value = 0.1493384940327061, Alternative = Port 4 Value = 0.1459123605216895,

Alternative= Port 5 Value = 0.16123691625555267 Alternative= Port 6 Value = 0.0881620903178278

In order calculate the best remaining portfolio I have implemented AHP, which can calculate up to 5 objectives and 20 alternatives, with the result shown in figure 17. From this valuation portfolio 2 $x = (1, 1, 0, 0, 1, 0, 1, 1, 1)$ should be chosen.

Figure 17: Case Study: AHP Calculator

This shows the great advantage of AHP. AHP can be used in various decision making problems. Mostly when the decision maker has to decide between alternatives with similar results or mostly when the decision maker has to express intangible measures into numbers. The drawback of this methodology is the high effort of valuing the alternatives with each other. Therefore AHP is recommended only for a limited number of alternatives (< 10) based on this case study.

7.7 Multi-Objective Security Safeguard Selection Tool

The aim of this section is to apply MOST [75] for the process based valuation of IT (security) investments. It will show how this approach can be applied in order to value the 6 remaining IT investment alternatives of section 8.5 considering the necessary safeguard selection of each IT investment alternative.

In the first step of MOST it is necessary to define, and value the cost and benefit categories for the safeguards. The benefit categories in this case are confidentiality, integrity, and availability. For simplicity the cost categories are: Implementation costs, Running Costs.

Intangible benefit categories like confidentiality, integrity, availability, can be valued with methods like AHP or the Swing Method (e.g Butler [86]). The benefit of this process based approach lies in the estimation of those values by deriving them from the business process. The benefit criteria *availability* can be computed by the downtime of the system using the values of table 15. For example if a system crash occurs, the automated process is not available for one day, then the value for Availability of IS 1 75\$. The benefit integrity can be seen in this case as a delay of performing this process. The objective confidentiality in this case is valued relatively low, because it is assumed, that for example money transactions are executed by a different business process. Note that this can only be average values. For example costs to reinstall the system are different if it was hit by a virus, or if it had a hard disc crash. The estimated values are shown in table 20.

VAL(a,b)	Availability	Integrity	Confidentiality
Accounting Process	165	80	40

Table 20: Case Study: Cost estimates for safeguards

This table further shows, that for simplicity only one asset is considered in this case study, namely the core business process. A more detailed case study would subdivide this process, into smaller parts, to value each sub process exclusively.

The definition of a risk is modified by adding IT investment alternatives into the definition of a risk. IT is extended to:

$$R = A \times IT \times V \times T \times \rightarrow \mathbf{R} \quad (33)$$

This extension implies that a security breach only occurs, if a threat (hacker) exploits a vulnerability (open ports), from an IT system (IT 1), and causes harm to an asset (business process). In this case risks are generated through the cartesian product of the IT alternative, vulnerability and threats. Only if an IT alternative offers a vulnerability, which can be exploited by a threat, the decision maker faces a risk. Note that not all combinations are sensible. The risks associated in this case are shown in figure 18 with their Annual Rate of Occurrence, and the Exposure Factor shown in table 21.

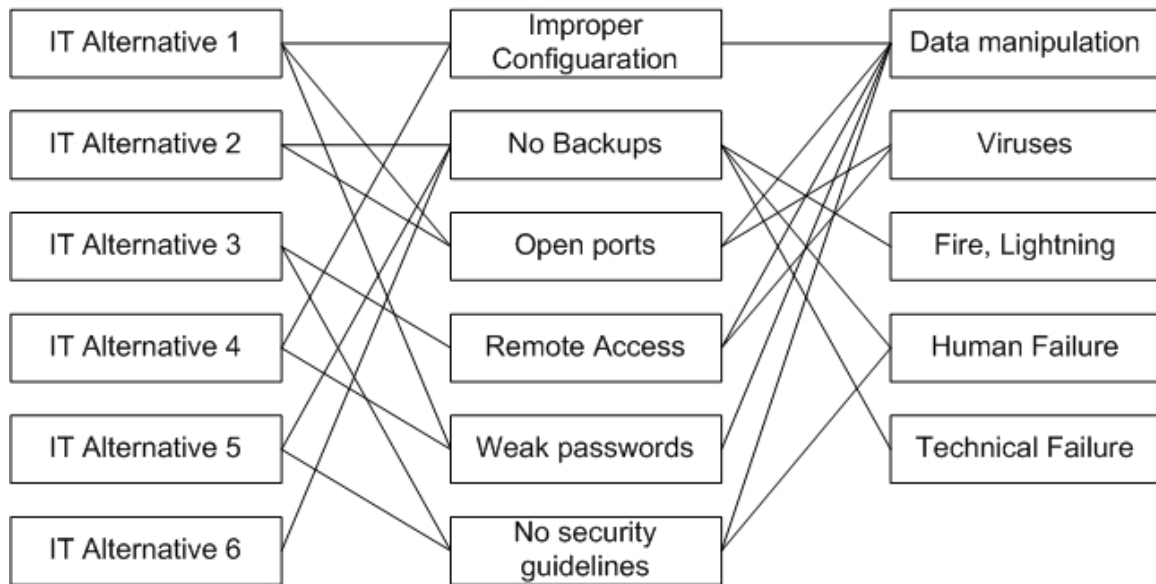


Figure 18: Case Study: Risks for MOST

Risk(IT,vulnerability,threat)	ARO	EXF(r,a)	EXF(r,i)	EXF(r,c)
$R_{A1,IC,DM}$	2	0.1	0.6	0.2
$R_{A1,OP,DM}$	4	0.2	0.8	0.3
$R_{A1,OP,V}$	8	0.7	0.4	0.1
$R_{A1,WP,DM}$	1	0.6	0.75	0.2
$R_{A2,NB,FL}$	0.2	0.9	0.05	0
$R_{A2,NB,HF}$	6	0.4	0.5	0
$R_{A2,NB,TF}$	20	0.95	0.1	0
$R_{A2,OP,DM}$	4	0.2	0.8	0.3
$R_{A2,OP,V}$	8	0.7	0.4	0.1
$R_{A3,RA,DM}$	3	0.7	0.8	0.6
$R_{A3,RA,V}$	11	0.6	0.5	0.2
$R_{A3,NSG,HF}$	8	0.3	0.2	0.3
$R_{A3,NSG,DM}$	4	0.2	0.6	0.4
$R_{A4,IC,DM}$	2	0.1	0.6	0.2
$R_{A4,WP,DM}$	15	0.6	0.75	0.25
$R_{A5,IC,DM}$	2	0.1	0.6	0.2
$R_{A5,NSG,DM}$	8	0.2	0.6	0.3
$R_{A5,NSG,HF}$	4	0.3	0.2	0.4
$R_{A6,NB,FL}$	0.2	0.9	0.05	0
$R_{A6,NB,HF}$	6	0.4	0.5	0
$R_{A6,NB,TF}$	20	0.95	0.1	0

Table 21: Case Study: Risks and Annual Rate of Occurrence

The next step results in defining the safeguard alternatives, their interactions, and their according cost/benefit estimates. These estimates are shown in table 22.

Each safeguard has a specific effectiveness to reduce the vulnerability. Those estimates are shown in table 23.

Safeguards	Implementation costs	Running Costs
Configuration Checklist	150	120
Firewall	300	20
Security Guidelines	200	20
Restricted Remote Access	50	80
Backups	20	300
Password Policy	250	20
Anti Virus Program	100	100

Table 22: Case Study: Cost estimates for safeguards

EFF(s,v)	EFF(availability)	EFF(integrity)	EFF(confidentiality)
$EFF_{CC,IC}$	0.4	0.4	0.2
$EFF_{FW,OP}$	0.3	0.7	0.7
$EFF_{SG,NSG}$	0.25	0.4	0.3
$EFF_{RMA,RA}$	0.3	0.85	0.6
$EFF_{B,NB}$	0.95	0.4	0.05
$EFF_{PWP,WP}$	0	0.8	0.3
$EFF_{AV,IC}$	0.1	0	0.2
$EFF_{AV,OP}$	0.65	0.35	0.2
$EFF_{AV,NSG}$	0.4	0.25	0.1

Table 23: Case Study: Effectiveness of safeguards

Compared to MODS for IT investment this model is more complex. Especially the valuation is more challenging to implement. The source code is provided in Appendix E for a comparison. Due to this benefit/Cost categorization the algorithm finds a lot of pareto efficient solution. For example there are 83 for IT 1. Therefore the algorithm was modified to find the portfolio solution with minimized security costs. Security costs in this case is defined as the ALE + Cost categories. The solution is shown in table 24.

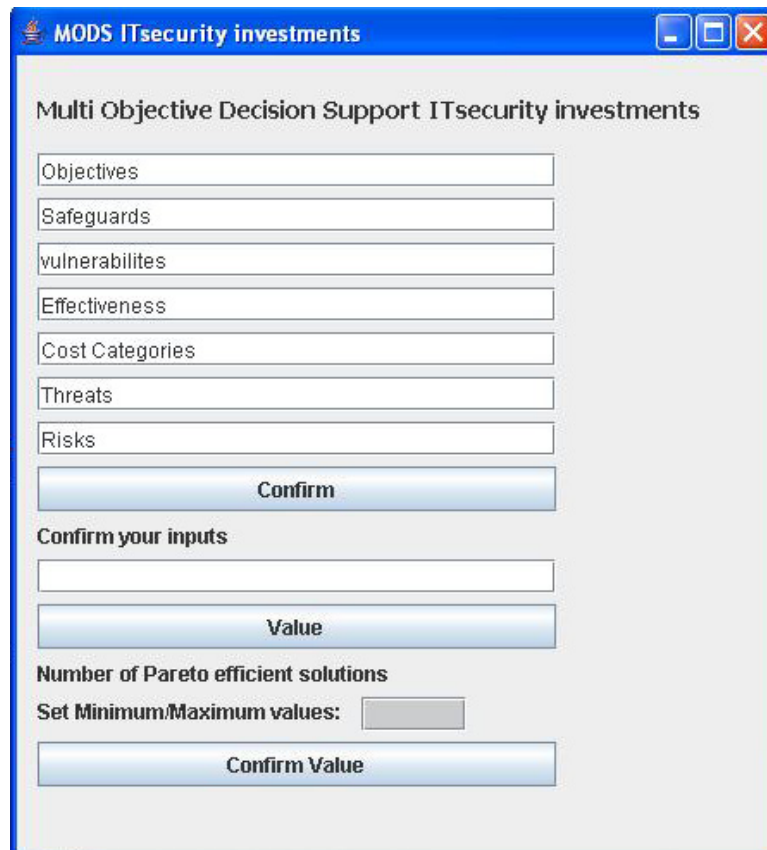
IT alternative	ALE(A).	ALE(I)	ALE(C)	ALE(A)w.S	ALE(I)w.S	ALE(C)w.S	IC	RC	SC
IT 1 (0100001)	1187	668	104	216	215	34	400	120	986
IT 2 (0100101)	4617	912	80	266	300	13	420	420	1419
IT 3 (0010001)	1964	952	320	1640	728	246	300	120	3035
IT 4 (0000010)	1518	996	166	1518	276	121	250	20	2185
IT 5 (0000001)	495	544	176	189	282	99	300	120	989
IT 6 (0000100)	3561	401	0	178	240	0	20	300	739

Table 24: Case Study: Solution Most

The first three columns show the ALE without a safeguard, and the last column shows the summed up security costs. Note that this sum derives from regular and one time expenses. So these are the security costs for one year. According to this solution IT 6 with the safeguard *Backups* should be chosen.

This solution further shows the high variation of costs, which may derive from different IT investment alternatives. This concludes on the importance of valuing an IT

investments, considering security costs.



The image shows a software window titled "MODS ITsecurity investments". The window contains a form for "Multi Objective Decision Support ITsecurity investments". The form has several input fields: "Objectives", "Safeguards", "vulnerabilites", "Effectiveness", "Cost Categories", "Threats", and "Risks". Below these fields is a "Confirm" button. Underneath is a section titled "Confirm your inputs" with an empty input field and a "Value" button. Below that is a section titled "Number of Pareto efficient solutions" with the text "Set Minimum/Maximum values:" followed by a small grey input field and a "Confirm Value" button.

Figure 19: Case Study: MOST Calculator

7.8 Summary

This section showed how IT investments can be valued based on the categorization in *low*, *medium*, and *high* risk IT investments, with Cost/Benefit Analysis, Real Option Valuation, Multi-Objective Decision Support, and the Analytical Hierarchy Process. The remaining IT investment alternatives from this calculation were valued with a modified approach of the Multi-Objective Security Safeguard Selection Tool. With this approach it is possible to value IT investment alternatives considering the appropriate level of IT security investments. The solution suggests the importance of considering security costs during the IT investment valuation, due to the high variations of security costs between IT investment alternatives. In addition the advantages of a process based valuation of IT security were experienced, by the improvement of estimating input variables for MOST. In addition it showed the major advantage of MOST, which is the consideration of multiple safeguards which, reduce the same vulnerability. The drawback of this approach is high effort of calculating time, when many alternatives have to be considered. This stands for the implementation of metaheuristic procedures like Ant Colony Optimization, Non Dominated Genetic Algorithms, . . . instead of complete enumeration to improve this process.

8 Elaboration on Research Questions

This section elaborates on the research question presented in 1.2. It focuses on the evaluation, and not on the case study of this thesis, because the aim of this thesis was to evaluate the differences between IT and IT security investments. The presented approach used in the case study derives from the results of this evaluation.

What are the differences between IT and IT security investments?

Definition/Aim: The aim of an IT (security) investment is a positive relationship between spending on IT or in IT security with resulting benefits or effectiveness. While these benefits of IT investments derive from increased cashflows, the benefits of IT security investments stem from reduction of possible losses due to security breaches. In particular positive return of IT security is measured in the reduced Annual Loss Expectancy over the security costs.

Planning: The planning of an IT investment begins on top of an organization, where possible improvements of external relationships, organizational environment, business processes, and the existing IT infrastructure with an IT investment are estimated, and calculated with valuation methods. In addition possible risks, which can reduce the benefits of an IT investment are derived from these components and valued in the risk management process. The planning of IT security takes place within the risk management process. It is referred to the management of technology risk factors. It starts with the *risk assessment process*, where possible risks are generated and valued. In order to prevent risks from happening IT investment alternatives (safeguards) are generated, and calculated with valuation methods in the *risk mitigation process*.

Challenges: The first and major challenge for both fields can be put in the category "Estimating tangible and intangible costs and returns" of the investment. This thesis concludes from its research, that this problem has the following differences and commonalities in both fields: 1) IT directly affects the business process, which makes it possible to accurately estimate returns with business process management tools like *Adonis*. For IT security investments such a comparable process based approach to value IT security investments is missing. 2) Both investments can have impacts on many areas of the organization. This leads to the next challenge "Lack of Information" The challenge is referred to the estimation of input variables, which are connected to uncertainty about future outcomes. While in the field of IT investments these input variables are only part for the valuation, IT security valuation methods close to exclusively face these input variables. Due to this challenge multiple objectives have to be considered in order to align the IT and IT security investment to the organization's strategic drivers. "Many Alternatives"

Both fields face a vast number of investment alternatives, which have to be valued. The reason for IT investments is that the return can be maximized by altering existing business processes, which makes individual software solutions necessary. In a complex system there are numerous things, that can go wrong and nearly as much safeguards to prevent risks from occurring. This makes portfolio selection of investment alternatives necessary in both fields. "Time perspective" For every investment the time value of money, and the resulting returns have to be framed within a time perspective. The time frame has strong influences on the solutions of valuation methods of IT investments. The problem of introducing a time perspective for IT security investments is shown by the following example, which applies the Net Present Value for IT security investments, face risks with low annual rate of occurrence, and a high asset value:

For example an information organization like *Reuters*, which produces IT systems, and information concerning the financial market for their costumers. What happens if somebody could hack into this information system, and put in framed information (e.g. U.S. President is dead), the objective (confidentiality) would not be achieved, and further result in a devastating loss for the organization and their costumers. The following simple example is hypothetical only and does not reflect the organizations real numbers: $ARO = 0.1$, $SLE = 1.000.000.000\$$ $EF = 100\%$ $RM = 99\%$ and the $CSI = 10.000.000\$$. Calculating the ROSI would still be positive: $ROSI = \frac{(100.000.000 * 0.99) - 10.000.000}{10.000.000} = 890\%$. In contrast there is an alternative in investing a firewall which reduces this risk by 40% and costs only 10.000\$ would result in a much higher Return on Security value: $ROSI = \frac{(100.000.000 * 0.40) - 1.000.000}{1.000.000} = 3900\%$. Although it is clear in this example, that the first alternative should be chosen, the ROSI methodology recommends the second alternative. This makes one point clear: ROSI lacks of valuing such risks, which leads to the insight that there is the need of a differentiation of such risks. This may result in a criterion like $ARO < 1$ and $SLE > x$, where $x \in \mathbf{R}$. The problem which arises from such risks is the time perspective. The Return of our Investment depends on when the attack occurs. This is shown by using the NPV for this example, if the hack occurs after the first year of the installation of the safeguard:

$$NPV = -10.000.000 + 100.000.000 * 1.1^{-1} = 19.090.909\$ \quad (34)$$

If the hack occurs after 5 years of the installation of the safeguard:

$$NPV = -10.000.000 + 100.000.000 * 1.1^{-5} = 7.209.213\$ \quad (35)$$

This difference would be even higher if we would consider maintenance costs for the security safeguard. This example makes clear that we have to differentiate between risks, and introducing a sense full time perspective for IT security investments. Table 25 sums up these challenges (c.f. section 2,3 for a detailed discussion).

Challenges IT investments	Challenges IT-Security Investments
Many Alternatives [30] [74] [85]	Many Alternatives [14] [15]
Lack of Information [30] [24] [85]	Lack of Information [42] [54] [21]
Intangible Costs/Returns [85] [67]	Intangible Costs/Returns [68] [40]
Multiple Objectives [85] [30] [74]	Multiple Objectives [84], [6], [64]
Time perspective [16] [60]	Narrow View on Risks [21]
	Time Perspective

Table 25: Challenges for IT and IT-(Security) Investments

What processes, from a psychological point of view, influence in what way the result of a subjective estimation of input variables?

People rely on a restricted figure of heuristic principles that shrink the complex tasks of assessing possibilities and calculating values to simpler judgmental operations which seldom lead to systematic errors. Major heuristics are *Representativeness*, *Availability*, *Adjustment* and *Anchoring*.

The representativeness heuristic can lead to misinterpretation of the expected value. The availability heuristic influences the probability estimation by the occurrences that can be brought to mind. The adjustment and anchoring heuristics can lead to overestimation of the probability of conjunctive events which lead to unwarranted optimism in the evaluation of the likelihood that a project will succeed or completed on time. On the other hand due to anchoring people will tend to underestimate the overall probabilities for failure in complex systems.

All in all there are many sources of error, when input variables are estimated subjectively (c.f. Tversky [102] for a detailed discussion). This leads to following conclusions: 1) Importance of improving the estimation of input variables for IT and IT security investments 2) Awareness of decision makers of these heuristics.

What are the differences between valuation methods of both fields?

Criteria	Return on Investment	Return on Security Investment
Challenge(s)	Intangible Cost/Returns Time Perspective	Intangible Cost/Returns
Formula	$ROI = \frac{profit}{investment_cost}$	$ROSI = \frac{(ALE*RM)-CSI}{CSI}$
Input Variable(s)	Costs Benefits time	Cost Risk Mitigated Annual Loss Expectancy

Table 26: Difference between ROI and ROSI

Table 26 contrasts the Return on investment of IT investments with the Return on Security investments. Both metrics result in a Cost/Benefit ratio. The difference lies within the type Cost and Benefits. They can come from various sides IT investments. Therefore it is vital for a ROI analysis to perform an extensive analysis, which catches all tangible/intangible costs and benefits. In addition a sophisticated ROI calculation includes the time value of money. In contrast, benefits for the Return on Security investments derive from the risk which is mitigated by the IT security investment (safeguard). The value of this mitigation depends on the value of the underlying asset, which is derived from the Annual Loss Expectancy (ALE). Investing in safeguard(s) result in minimizing those costs, which is the benefit of the investment. The challenging part of this calculation lies within estimating the ALE. This variable depends on two criteria, which are difficult to estimate: The costs, which occur from a successful attack, and the probability of a successful attack. For a sophisticated estimation of those potential costs it is vital to understand the strategic, business role of the IT system. Estimating the risk mitigation depends mostly on subjective estimates.

Due to the different input variables the solution of those Cost/Benefit ratios have to be differently interpreted. While ROI can not get negative, and a positive return of is considered with a value above 100%, ROSI can get negative, and is considered as valuable when it gets positive.

Table 27 takes a closer look on ROI and ROSI by comparing input variables of Cost/Benefit analysis and Real Option Valuation for IT investments with Defense Trees and Return on Security from Mizzi. This table shows that Real Option valuation considers a project's uncertainty in form of volatility compared to common Cost/Benefit analysis. Further it requires more than one cashflow, because it calculates the option value considering multiple cashflow expansions. Although this can be performed with Cost/Benefit Analysis, as well, which is commonly referred to *Sensitivity Analysis* to get a mean value, this approach is mandatory to perform a meaningful Real Option Valuation.

Table 28 compares more sophisticated methodologies of IT and IT security investments with special focus on Multiobjective Decision Support Systems. It shows, that IT investments are strongly linked to the business process(es). In contrast, a suitable IT security

CBA(IT)	ROV(IT)	DefenseTrees(SEC)	Mizzi(SEC)
Benefits	Benefits	Single Loss Expectancy	Instantaneous Loss
Costs	Costs	Annual Rate of Occurrence	value information asset
Cashflow	Cashflows	Risk Mitigated	Annual costs to fix vulnerabilities
time	time until opportunity	Cost Safeguard	One time cost
interest rate	interest rate	Expected Gain Hacker	maintenance costs
	project uncertainty	Cost of Attack	instantaneous loss
			time system is down
			cost to rebuild system
			costs to break into system
			costs to exploit vulnerabilities
			damage to defense mechanisms
			& infrastructure

Table 27: Difference between CBA(IT),ROV(IT),ROSI(SEC)

AHP(IT/SEC)	MODS(IT) [74]	AEM(SEC) [86]	MODS(SEC) [75]
	Set of business processes		
benefit criteria	benefit criteria	outcome attributes	Assets
	units	outcome attribute values	vulnerabilities
Set of IT alternatives	Set of IT alternatives	ranking outcome attributes	threats
		frequency of attack	ARO (frequency)
		IT security categories	IT security categories
		risk mitigation	risk mitigation
		objectives	objectives
		safeguard costs	safeguard costs
			safeguard interactions

Table 28: Difference between MODS (IT) AEM(SEC) MODS (SEC)

investment depends on assets, vulnerabilities, and threats, which can lead to 1) Execution of the according business process(s) is deferred/stopped for a period of time, and 2) Result in serious effects on the strategic performance of the organization, depending on the type of the damage (Confidentiality, Integrity, Availability, Authenticity). This results in different thinking of costs and benefits between those fields. While decision makers of IT investments are concerned how they can speed up business processes or change existing business processes with IT systems in order to improve the strategic performance of the organization, decision makers of IT security investments have to think about the various effects, which can go far beyond the delay of existing business processes. For example if an attacker hacks into the customer database of a bank and gets the *TANs* (Confidentiality) of the customers, this would most probably not have any effects on the business processes, but have effects on the *customer satisfaction*, and further result in a serious loss of money. This difference in thinking about IT and IT security investments leads 1) To more input variables, 2) To more complex IT security investment valuation methods, 3) To a higher amount of proposals of IT security investment methodologies.

At this point it is necessary to add that the scope of this thesis is limited, because the most challenging part of decision making for IT investments lies in generating, and altering business processes according to the strategic drivers of an organization with suitable IT systems. This requires skills in understanding the economics of organizations, and knowing about the capabilities of information technology.

While ROI and ROSI or Multiobjective Decision Support for IT and IT security investments can be directly compared (AHP can be used in both fields), for Real Option Valuation there is not a comparable IT security investment methodology. The question which arises from this aspect is "Is possible to adopt Real Option Valuation for IT security investments?" The most obvious problem is the difference in thinking about *the time perspective* of uncertainty and risks. This can be explained by the following example: If somebody is considering buying a PC and a printer. In the classic NPV approach he would calculate the NPV by the rate of return when investing in the PC and printer in the present. The Real Options approach modifies this thinking in: First he invests in the PC and two months later he defines the option of buying a printer depending on how much pages he actually needs to print and on the future prices of a copy shop. This option to defer the investment of the printer has a flexibility value, which is considered in the Real Option Valuation. Due to the difference of sources of Costs and Benefits between IT and IT security investments this valuation seem unsuitable for IT security investments. For example if a burglar wants to steal a home PC, it would be necessary to consider a time perspective: When is best time to invest in a better door which holds the burglar off the home? In order to apply Real Option it would be necessary to know *when* the burglar most probably would try to steal the PC. Whereas this reason should not lead to the insight that applying Real Options on IT-Security Investments is not sense full. At the time of writing there was one approach, to find which uses real option valuation for IT security investments (e.g.[45]), where the author states "Although this wait-and-see approach toward information security expenditures may seem unwise on the surface, there is a rational economic explanation for such an approach under the appropriate conditions." Unfortunately it was not possible to get insight into this paper.

Challenge	IT				IT security		
	CBA	ROV	AHP(IT/SEC)	MODS [74]	DT [14]	AEM[86]	MOST[75]
Many Alternatives			X	X			X
Lack of Information		X	X	X		X	X
Intangible Costs/Returns	X	X	X	X	X	X	X
Multiple Objectives			X	X		X	X
Time Perspective	X	X	X	X			

Table 29: Challenges addressed by valuation methods

Table 29 shows the challenges addressed by each methodology. Whereas, this table does not reflect how *good* these challenges are solved by each methodology.

Note that some approaches directly address the use of a *Sensitivity Analysis*. A Sensitivity Analysis can be used to value the degree of error. There are many variations to performing sensitivity analysis, but a common way is to select costs, benefits, or other parameters in the calculation, which are assumed to have uncertain values, and vary them in order to check their effects [85]. This stands basically for all methodologies and was therefore not considered as benefit in this evaluation.

The evaluation concludes, that only *Time Perspective* and *Intangible Costs/Returns* are addressed by Cost/Benefit Analysis. Their strength lies in their simple concept, which can give suitable solutions for low risk investments. Although, tangible and intangible costs and returns can be included if a serious Cost/Benefit Analysis was performed, they can give a misleading indication, because "intangible costs and returns are downsized to a single value" [74].

Real Option Valuation addresses the challenges *Intangible Costs/Returns*, *Time perspective*, and *Lack of Information*. Real Options are very suitable for IT investments, which depend strongly on market positions and aspirations. In fact, up to 60 percent of IT investments depend on its market position and aspirations [28]. It focuses on the strategic planning phase of an IT investment, which leads to flexibility and increased responsiveness, by considering multiple forms of risk, and incomplete information [97]. The lack of this methodology is the difficulty of estimation the input variables for this method.

With AHP it is possible to address all challenges. The reason for this lies in the fact, that AHP is adoptable for various decision making problems (example for security: Bodin [15]). Therefore the decision maker can individually adopt AHP for the specific decision making problem. This is basically done by translating strategies into objectives and measures. But it lacks of the high effort of the pairwise comparison of IT (security) investment alternatives.

Multiobjective Decision Support directly addresses the challenge *Many Alternatives* in a way, which no of the other methods is capable of. It considers the aspect, when the decision maker has to decide among alternatives, which have similar or same functionalities. This changes the way of thinking of "Should I invest in A or B or C?", to "Should I invest

in A and/or B and/or C?”. This creates a portfolio of investment alternatives, where in addition individual dependencies and properties of alternatives can be considered. Further MODS addresses *Lack of Information*, where compared to AHP, less a-priori information is needed, because the decision maker can individually change/set boundaries, in order to see how these changes effect the solution space. The valuation of Neubauer’s [74] approach is strongly linked to organization’s strategy, business process, multiple objectives, and resource constraints.

These advantages get even stronger for IT security investments. For example: Often a countermeasure can mitigate more than one attack/risk. The ROSI can be completely different, because the RM depends on the specific attack and the ALE can be different depending on the attack. Defense Trees lack of the consideration of this aspect. Although the Security Attribute Evaluation takes this lack under consideration, by implementing the Technology Index, it is not possible to consider multiple safeguards, which take care of the same vulnerability. This aspect has to be solved through portfolio analysis of safeguards, where MOST comes into play, by implementing the aggregated effectiveness of multiple safeguards.

9 Conclusion

In the past decade organizations overspent a lot on IT, which stands for IT, and IT security investments. The reasons why this has occurred are 1) Organizations have missed to achieve a competitive advantage by concentrating on speeding up their current business processes, and 2) The missing alignment of IT security to the organization's strategic drivers due to technology centric approaches.

Studies revealed that organizations, which classified their IT investment into *low*, *medium*, and *high* risk IT investments got a positive return out of their spending in IT. In particular, this classification involves the differentiation of IT investments which 1) Improve existing business processes, and 2) Alter existing business process in order to gain a competitive advantage. The second category makes the valuation of individual software solutions necessary, which results in a large amount of IT investment alternatives. They have to be evaluated, considering their functionality, effectiveness and dependencies.

Decision makers of IT security investments face a similar challenge. It is close to impossible to create a complete list of things that can go wrong in (complex) IT systems. Therefore the decision maker has to decide among a vast number of safeguards, which may reduce the same vulnerability, with different dependencies and effectiveness. This results in a high demand on valuation methods, which have to consider this complexity.

This argument stands for Multiobjective Decision Support Systems in both fields. With them it is possible to value IT and IT security investment alternatives, which have the same functionality, considering the organization's objectives with a process based approach.

The case study showed how *Cost/Benefit Analysis*, *Real Option Valuation*, *Analytic Hierarchy Process*, and *Multi Objective Decision Support* can be appropriately applied depending on the classification of the IT investment with a business process based approach. It continued with the valuation of possible safeguards for the IT investment alternatives with a modified version of MOST. The case study showed 1) The improvement of estimating input variables for IT security investments, due to the process based approach. 2) The advantages of valuing IT security investment alternatives within the valuation of IT investments.

Future Work will focus on 1) The Improvement of MODS with metaheuristic procedures like Ant Colony Optimization, Non Dominated Genetic algorithms . . . to reduce the calculation time of MODS. 2) Applying MODS for Real Option Valuation to consider interactions between options, and 3) Further improving the estimation of input values for IT security investments. As Soohoo [90] states this problem to the point "A model is only as good as the information put into it".

Acknowledgements

I would like to thank:

- Thomas Neubauer for his support during the time of writing this thesis. I want to thank him especially for being the source of new ideas, and for pushing me where I would not have gone by myself.
- Alexander Peretti for supporting my early interest in computers.
- All of my friends, especially Reinhard Mühlwerth and Martin Stubenschrott, for making my studies an interesting and very entertaining experience.
- Christoph Slezak for reading this thesis to minimize mistakes.
- Daphne, Elisabeth and Kimon Vafiadis for their encouragement.
- My family Claudia, Thomas, Csilla and Ingmar Hartl for their mental and financial support.

References

- [1] AL-HUMAIGANI, M., AND DUNN, D. A model of return on investment for information systems security. *Department of Electronics and Computer Technology* (2004).
- [2] ALPCAN, T., AND BASAR, T. A game theoretic approach to decision and analysis in network intrusion detection. *Proceedings of the 42nd IEEE Conference on Decision and Control 3* (2003), 2595–2600.
- [3] AMICO, M., AND PASEK, Z. A new methodology to evaluate the real options for an investment using binomial trees and monte carlo simulation. *Proceedings of the Winter Simulation Conference* (2003), 351–359.
- [4] AMRAM, M., AND KULATILAKA, N. *Real Options: Managing Strategic Investment in an Uncertain World*. Harvard Business School Press, 1999.
- [5] ANDERSON, B. *The Three Secrets of Wise Decision Making*. Single Reef Press, 2002.
- [6] ANDREWS, M., AND WHITTAKER, J. Computer security. *IEEE: Security & Privacy Magazine 2* (2004), 68–71.
- [7] *APPEL, A., ARORA, N., AND ZENKICH, R. Unraveling the mystery of it costs. *McKinsey on IT 3* (2005), 12–17.
- [8] *APPEL, A., DHADWAL, A., DORGAN, S., AND DOWDY, J. When it creates value. *McKinsey on IT 4* (2004), 10–12.
- [9] BAR-HILLEL, M. *On the subjective probability of compound events*. *Organizational Behavior and Human Performance*, 1973, ch. 9, pp. 396–406.
- [10] BARDHAN, I., BAGCHI, S., AND SOUGSTAD, R. A real options approach for prioritization of a portfolio of information technology projects: A case study of a utility company. *Proceedings of the 37th Hawaii International Conference on System Sciences* (2004).
- [11] BELL, D. Regret in decision making under uncertainty. *Operatoins Research 30* (1982), 961–981.
- [12] BENAROCH, M. Managing information technology investment risk: A real options perspective. *Journal of Management Information Systems 9* (2002), 43–84.
- [13] BENAROCH, M., AND KAUFFMAN, R. A case study for using real options pricing analysis to evaluate information technology project investments. *Information Systems Research 10* (1999), 70–86.

- [14] BISTARELLI, S., FIORAVANTI, F., AND PERETTI, P. Defense trees for economic evaluation of security investments. *IEEE-Proceedings of the First International Conference on Availability, Reliability and Security (ARES 06)* (2006).
- [15] BODIN, L., GORDON, L., AND LOEB, M. Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM* 48 (2005), 79–83.
- [16] BOER, P. Real options: The it investment risk buster. *Information Week's Optimize* (2002).
- [17] BREMAUD, P. *Markov Chains*. Springer Science and Business Media, 1999.
- [18] BUTLER, S., AND PAUL, F. Multi-attribute risk assessment. Tech. rep., CMU-CS-01-196, 2001.
- [19] BUTLER, S., AND SHAW, M. Incorporating nontechnical attributes in multi-attribute analysis for security. *Position Paper for the Fourth Workshop on Economics-Driven Software Engineering Research (EDSER-4)* (2002), 45–48.
- [20] *BUZZARD, K. Computer security - what should you spend your money on? *Computer & Security* 18 (1999), 322–334.
- [21] *CARALLI, R., AND WILSON, W. The challenges of security management. *CERT Coordination Center* (2004).
- [22] CAVUSOGLU, H., MISHRA, B., AND RAGHUNATHAN, S. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce* 9 (2004), 69–104.
- [23] CLARKE, R., AND STEVENS, K. Evaluation or justification? the application of cost/benefit analysis to computer matching schemes. *Proceedings of European Conference on Computer Systems (ECIS'97)*, 1997 available at: <http://www.anu.edu.au/people/Roger.Clarke/SOS/ECIS97.html> (1997).
- [24] CLEMONS, E., AND WEBER, B. Strategic information technology investments: Guidelines for decision making. *Journal of Management Information Systems* 7 (1990), 9–28.
- [25] COBB, B., AND CHARNES, J. Simulation and optimization for real options valuation. *Proceedings of the Winter Simulation Conference* (2003), 343–350.
- [26] COHEN, J., CHESNICK, E., AND HARAN, D. A conformation of the inertial effect in sequential choice and decision. *British Journal of Psychology* 63 (1972), 41–46.

- [27] CORBETT, R. A view of the future of risk management. *Risk Management: An International Journal* 6(3) (2004), 51–56.
- [28] *CRAIG, D., AND TINAIKAR, R. Divide and conquer: Rethinking it strategy. *McKinsey on IT* 3 (2006), 4–13.
- [29] CREMONINI, M., AND MARTINI, P. Evaluating information security investments from attackers perspective: The return on attack. *4th Workshop on the Economics on Information Security* (2005).
- [30] CRESSWELL, A. Return on investment in information technology: A guide for managers. *Center for Technology in Government University at Albany* (2004).
- [31] DAVENPORT, T. *Process Innovation: Reengineering Work Through Information Technology*. Harvard Business School Press, 1993.
- [32] DAVIS, G. Estimating volatility and dividend yield when valuing real options to invest or abandon. *The Quarterly Review of Economics and Finance* (1998), 725–754.
- [33] DOROFEE, A., WALKER, J., HIGUERA, R., MURPHY, R., AND WILLIAMS, R. *Continuous Risk Management Guidebook*. Carnegie Mellon Software Engineering Institute, 1996.
- [34] DUNCAN, W. *A Guide to the Project Management Body of Knowledge*. Project Management Institute Publications, 1996.
- [35] DWAIKAT, Z., AND PARISI-PRESICCE, F. Risky trust: risk-based analysis of software systems. *International Conference on Software Engineering: Proceedings of the 2005 workshop on Software engineering for secure systems* (2005), 1–7.
- [36] ECKERT, C. *IT-Sicherheit: Konzept-Verfahren-Protokolle*. Oldenbourg Verlag, 2004.
- [37] ELFARISSI, I., SAHUT, J.-M., AND BELLALAH, M. Evaluation of real options with information costs. *The Financial Review* (2002).
- [38] *FARRELL, D., TERWILLIGER, T., AND WEBB, A. Getting it spending right this time. *The McKinsey Quarterly* 2 (2003), 118–129.
- [39] FISCHHOFF, B., SLOVIC, P., AND LICHTENSTEIN, S. Fault trees: Sensitivity of estimated failure probabilities to problem representation. *Journal of Experimental Psychology: Human Perception and Performance* 4 (1978), 330–334.

- [40] FOSTER, S., AND PAUL, B. Analysis of return on investment for information security. Tech. rep., Getronics Inc., 2002.
- [41] GAO, F., SUN, J., AND WEI, Z. The prediction role of hidden markov model in intrusion detection. *IEEE-Canadian Conference on Electrical and Computer Engineering* (2003), 893–896.
- [42] GAO-ACCOUNTING, AND DIVISION, I. M. Information security risk assessment-practices of leading organizations, Nov 1999.
- [43] GARDNER, L. Using information generated by a discrete event simulation to evaluate real options in a research and development environment. *Proceedings of the Winter Simulation Conference* (2000), 2040–2047.
- [44] GORDON, L. Economic aspects of information security in a netcentric world. *Secure-Biz CxO Security Summit* (2004).
- [45] GORDON, L., LOEB, M., AND LUCYSHYN, W. Information security expenditures and real options: A wait-and-see approach. *Computer Security Journal* 19 (2003), 1–7.
- [46] GOSH, J., MOHAN, D., AND SAMANTA, T. *An Introduction to Bayesian Analysis. Theory and Methods*. Springer, Berlin, 2004.
- [47] GRENNEMEIER, L. Ninth annual global security survey. *Information Week* 9 (2006), 39–48.
- [48] HANSSON, S.-O. Decision Theory-A brief introduction. *Royal Institute of Technology (KTH)* (1994).
- [49] HARSANYI, J. Bayesian decision theory, subjective and objective probabilities, and acceptance of empirical hypotheses. *Synthese* 57 (1983), 341–365.
- [50] HERRMANN, G. Security and integrity requirements of business process - analysis and approach to support their realisation. *Proc. CAisE: 6th Doctoral Consortium on Advanced Information Systems Engineering* (1999), 36–47.
- [51] HERRMANN, G., AND PERNUL, G. Towards security semantics in workflow management. *Thirty-First Annual Hawaii International Conference on System Sciences* 7 (1998), 766.
- [52] HERRMANN, G., AND PERNUL, G. Viewing business process security from different perspectives. *International Journal of Electronic Commerce* 3 (1999), 89–103.

- [53] HERRMANN, G., RÖHM, A., AND PERNUL, G. Sichere geschäftstransaktionen auf elektronischen märkten. *Electronic Business Engineering / 4. Internationale Tagung Wirtschaftsinformatik* (1999), 188–207.
- [54] HILLSON, D., AND HULETT, D. Assessing risk probability : Alternative approaches. *PMI Global Congress Proceedings* (2004).
- [55] JABLONOWSKI, M. High-risk decision when probabilities are unknown (or irrelevant). *Risk Management: An International Journal* 6(4) (2005), 57–61.
- [56] JUNGINGER, S., KÜHN, H., STROBL, R., AND KARAGIANNIS, D. Ein Geschäftsprozessmanagement-Werkzeug der nächsten Generation-ADONIS: Konzeption und anwendung. *Wirtschaftsinformatik* 42 (2000), 392–401.
- [57] KANDA, T. Evaluation using ahp. *IEEE-Proceedings of the 2005 International Confernece* (2005), 449–454.
- [58] KARLSSON, J., AND RYAN, K. A cost-value approach for prioritizing requirements. *Software IEEE* 14 (1997), 67–74.
- [59] KAUFFMAN, R., AND LI, X. Technology competition and optimal investment timing: A real options perspective. *IEEE Transactions of Engineering Management* 52 (2005), 15–29.
- [60] KAUFFMANN, R., AND XIAOTONG, L. Technology competition and optimal investment timing: A real options perspective. *IEEE Transactions on Engineering Management* 52 (2005), 15–29.
- [61] KELLY, A. *Decision Making Using Game Theory: An Introduction for Managers*. Cambridge University Press, 2003.
- [62] KNORR, K., AND ROHRIG, S. Security requirements of e-business processes. In *I3E* (2001), pp. 73–86.
- [63] KULATILAKA, N., P.BALASUBRAMANIAN, AND STORCK, J. Using real options to frame it investment problem. *Applications to Decision* (1999).
- [64] LANDWEHR, C., BULL, A., MCDERMOTT, J., AND CHOI, W. A taxonomy of computer program security flaws. *ACM Computing Surveys* 26 (1994), 211–254.
- [65] LIAO, G.-Y., AND SONG, C.-H. Design of a computer-aided system for risk assessment on information systems. *IEEE 37th Annual 2003 International Carnahan Conference on Security Technology* (2003), 157–162.

- [66] LOOMES, G., AND SUDGEN, R. Regret theory: An alternative theory of rational choice under uncertainty. *Economic Journal* 92 (1982), 805–824.
- [67] LUCAS, H. *Information Technology and the Productivity Paradox: Assessing the Value of Investing in IT*. Oxford University Press, 1999.
- [68] MERCURI, R. Security watch - analyzing security costs. *Communications of the ACM* 46 (2003), 15–18.
- [69] MIZZI, A. Return on information security investment. are you spending enough? are you spending too much? *ITtoolbox Security* (2005).
- [70] MOONEY, J., GURBAXANI, V., AND KRAEMER, K. A process oriented framework for assessing the business value of information technology. *The Data Base for Advances in Information Systems* 27 (1996), 68–81.
- [71] NEMBHARD, H., AND AKTAN, M. Effect of implementation time of real options valuation. *Proceedings of the Winter Simulation Conference* (2002), 1600–1605.
- [72] NEUBAUER, T., AND HARTL, C. On the singularity of valuating IT-security investments. Tech. Rep. SBA-07-04-01, Secure Business Austria, March 2007.
- [73] NEUBAUER, T., KLEMEN, M., AND BIFFL, S. Business process-based valuation of it-security. *Proceedings of the 7th International Workshop on Economics-Driven Software Engineering Research EDSE'05* 30 (2005), 1–5.
- [74] NEUBAUER, T., AND STUMMER, C. Extending business process management to determine efficient it investments. *Applied Computing 2007 (Proceedings of the 2007 ACM Symposium on Applied Computing)* (2007), 1250–1256.
- [75] NEUBAUER, T., STUMMER, C., AND WEIPPL, E. Workshop-based multiobjective security safeguard selection. *IEEE-Proceedings of the First International Conference on Availability, Reliability and Security* (2006), 366–373.
- [76] NEUMANN, J., AND MORGENSTERN, O. *Theory of Games and Economic Behavior*. Princeton University Press, 1944.
- [77] NEWTON, D., STARK, A., AND WIDDICKS, M. *Real Option Calculator: Manual*, 2007.
- [78] PATE-CORNELL, M., AND NEU, J. Warning systems and defense policy: A reliability model for the command and control of u.s. nuclear forces. *Risk Analysis* 5 (1985), 121–138.

- [79] POBBIG, H. Von den kosten- zur wertorientierung: Tco versus roi. *IT-Management* 7/8 (2005), 21–27.
- [80] RAZ, T., AND HILLSON, D. A comparative review of risk management standards. *Risk Management: An international Journal* 7(4) (2005), 53–66.
- [81] REMENYI, D., AND BROWN, A., Eds. *Proceedings of the 13th European Conference on Information Technology Evaluation* (Genoa, Italy, September 2006).
- [82] RUDOLF BAER, P. Z. Wie misst man it-sicherheit. *HMD* 216 (2000), 67–77.
- [83] SAATY, T. *The Analytic Hierarchy Process*. McGraw Hill, 1980.
- [84] SCHECHTER, S. *Computer Security Strength & Risk: A Quantitative Approach*. PhD thesis, Harvard University Cambridge, 2004.
- [85] SCHNIEDERJANS, M., HAMAKER, J., AND SCHNIEDERJANS, A. *Information Technology Investment: Decision-Making Methodology*. World Scientific Publishing Co Ltd, 2004.
- [86] SHAWN, C.-B. A. Security attribute evaluation method, 2002.
- [87] SLOVIC, P., FISCHHOFF, B., AND LICHTENSTEIN, S. Accident probabilities and seat belt usage: A psychological perspective. *Accident Analysis and Prevention* 10 (1978), 281–285.
- [88] SLOVIC, P., FISCHHOFF, B., AND LICHTENSTEIN, S. *Facts versus Fears: Understanding perceived risk*. Cambridge University Press, 1993, ch. 33, pp. 463–489.
- [89] SLOVIC, P., AND LICHTENSTEIN, S. *Organizational Behavior and Human Performance: Comparison of Bayesian and regression approaches to the study of information processing in judgment*. 1971, ch. 6, pp. 649–744.
- [90] SOOHOO, K. How much is enough? a risk-management approach to computer security. *CRISP* (2000).
- [91] STONEBUMER, G., GOGUEN, A., AND FERINGA, A. Risk management guide for information technology systems. *National Institute of Standards and Technology* (2002).
- [92] STRAUSS, C., AND STUMMER, C. Multiobjective decision support in IT-risk management. *International Journal of Information Technology and Decision Making* 1 (2002), 251 – 268.

- [93] STUMMER, C., AND HEIDENBERGER, K. Interactive rd portfolio analysis with project interdependencies and time profiles of multiple objectives. *IEEE Transactions on Engineering Management* 50 (2003), 175–183.
- [94] SVENSON, O. Are we all less risky and more skillful than our fellow drivers? *Acta Psychologica* 47 (1981), 143–148.
- [95] TALLON, P., KAUFFMAN, R., LUCAS, H., WHINSTON, A., AND ZHU, K. Using real options analysis for evaluating uncertain investments in information technology: Insights from the icis 2001 debate. *Communications of the Association for Information Systems* 9 (2002), 136–167.
- [96] TEUFEL, S., AND SCHLIENGER, T. Informationssicherheit - wege zur kontrollierten unsicherheit. *HDM - Praxis der Wirtschaftsinformatik* 216 (2000), 18–31.
- [97] TRIGEORGIS, L. Real options and investment under uncertainty: What do we know? *National Bank of Belgium Research series 200205-3* (2002).
- [98] TURROFF, M., AND LINSTONE, H. *The Delphi Method: Techniques and Applications*. Addison-Wesley, 2002.
- [99] TVERSKY, A., AND KAHNEMAN, D. *A Subjective Probability: A Judgement of Representativeness*. *Cognitive Psychology*, 1972, ch. 3, pp. 430–454.
- [100] TVERSKY, A., AND KAHNEMAN, D. Availability: A heuristic for judging frequency and probability. *Cognitive Psychology* 5 (1973), 207–232.
- [101] TVERSKY, A., AND KAHNEMAN, D. Prospect theory: An analysis of decision under risk. *Econometrica* 47 (1979), 263–269.
- [102] TVERSKY, A., AND KAHNEMAN, D. *Judgment under uncertainty: Heuristics and biases*. Press syndicate of the University of Cambridge, 1993, ch. 1, pp. 3–20.
- [103] UNKNOWN. A risk management standard. *The Institute of Risk Management, The National Forum for Risk Management in the Public Sector, The Association of Insurance and Risk Managers* (2002).
- [104] UNKNOWN. Information technology investment management-a framework for assessing and improving process maturity. *GAO-Accounting and Information Management Division* (2000).
- [105] UNKNOWN. <http://www.bsi.de>, Aug 2006.
- [106] UNKNOWN. <http://www.commoncriteriaportal.org>, Aug 2006.
- [107] UNKNOWN. <http://www.defenselink.mil>, Aug 2006.

- [108] UNKNOWN. Crystal reference encyclopedia, Feb 2007.
- [109] VESELY, W., GOLDBERG, F., ROBERTS, N., AND HAASL, D. *Fault Tree Handbook*. U.S. Nuclear Regulatory Commission, Washington, D.C. 20555, 1981.

* **References marked with an asterisk indicate secondary literature.**

List of Figures

- 1 IT investment relations 14
- 2 Business processes 17
- 3 Planning steps 18
- 4 Planning IT security investments 26
- 5 Simple Risk Tree 27
- 6 Risk Assessment Activities [91] 28
- 7 Risk Mitigation Chart [91] 29
- 8 Evaluation: Real Options Approach [97] 54
- 9 Evaluation: AHP example 58
- 10 Evaluation: ROSI for "Steal Server" [14] 63
- 11 Case Study: Accounting Process 78
- 12 Case Study: Strategic Vision for Real Options 85
- 13 Case Study: First Stage of IT investment 87
- 14 Case Study: Future Cash Flows 88
- 15 Case Study: Real Options Calculator 89
- 16 Case Study: MODS Calculator 91
- 17 Case Study: AHP Calculator 94
- 18 Case Study: Risks for MOST 96
- 19 Case Study: MOST Calculator 98

List of Tables

- 1 Major Objectives for IT-(Security) Investments 34
- 2 DT: Payoff Table [85] 42
- 3 Evaluation: Cost/Benefit Analysis 51
- 4 Evaluation: Real Options 55
- 5 Evaluation: AHP: Pairwise comparisons of alternatives 56
- 6 Evaluation: Analytical Hierarchy Process (AHP) 58
- 7 Evaluation: Multiobjective Decision Support 60
- 8 Evaluation: Return on Security Investments 64
- 9 Evaluation: Defense Trees 65
- 10 Evaluation: Comparison of two quantitative ROSI methodologies 67
- 11 Evaluation: Mizzi’s Return on Security Investment 68
- 12 Evaluation: Security Attribute Evaluation Method 72
- 13 Evaluation: Multiobjective Decision Support 75
- 14 Case Study: Effort of accounting process without IT investment 80
- 15 Case Study: IT investment alternatives 81
- 16 Case Study: Included Components by each IT investment alternative 82
- 17 Case Study: Cost/Benefit Analysis 84
- 18 Case Study: Real Options Analysis 89
- 19 Case Study: MODS IT investments 92
- 20 Case Study: Cost estimates for safeguards 95
- 21 Case Study: Risks and Annual Rate of Occurrence 96
- 22 Case Study: Cost estimates for safeguards 97
- 23 Case Study: Effectiveness of safeguards 97
- 24 Case Study: Solution Most 97
- 25 Challenges for IT and IT-(Security) Investments 102
- 26 Difference between ROI and ROSI 103
- 27 Difference between CBA(IT),ROV(IT),ROSI(SEC) 104
- 28 Difference between MODS (IT) AEM(SEC) MODS (SEC) 104
- 29 Challenges addressed by valuation methods 106

Appendix A - Real Options Calculator

```
import JSci.*;

private void Calculation(java.awt.event.ActionEvent evt) {
// Real Option Calculation
    try
    {
    PV = Double.valueOf(jTextField1.getText()).doubleValue();
    X = Double.valueOf(jTextField2.getText()).doubleValue();
    T = Double.valueOf(jTextField3.getText()).doubleValue();
    intrate = Double.valueOf(jTextField4.getText()).doubleValue();
    votal = Double.valueOf(jTextField5.getText()).doubleValue();
    } catch (Exception e)
    {
    SolutionTextField.setText("Wrong_Input_or_Input_Missing");
    return;
    }
// Normal Distribution
    if(Distributiontype==0)
    {
    NormalDistribution prob = new NormalDistribution();

    d1 = (Math.log(PV/X)+(T*intrate+(votal*votal*T)/2))/votal*Math.sqrt(T);
    d2 = d1 - votal*Math.sqrt(T);

    Pd1 = prob.cumulative(d1);
    Pd2 = prob.cumulative(d2);

    ROV = PV * Pd1 - X* Math.exp(-intrate*T)*Pd2;

    if(ROV<0) ROV=0;

    String solution = String.valueOf(ROV);
    SolutionTextField.setText(solution);
    }

//Lognormal Distribution
    if(Distributiontype==1)
    {
    LognormalDistribution prob = new LognormalDistribution();

    d1 = (Math.log(PV/X)+(T*intrate+(votal*votal*T)/2))/votal*Math.sqrt(T);
    d2 = d1 - votal*Math.sqrt(T);

    try{
        if(d1<0 || d2<0)
        {
            //If d1 or d2 are negative get d1/d2 from input
            d1= Double.valueOf(d1textfield.getText()).doubleValue();
            d2= Double.valueOf(d2textfield.getText()).doubleValue();
        }
    }
    catch (Exception e) {}
    try{
    Pd1 = prob.cumulative(d1);
    Pd2 = prob.cumulative(d2);}
    catch (Exception e)
    {
        d1textfield.setText("d1="+d1);
        d2textfield.setText("d2="+d2);
        return;
    }
    ROV = PV * Pd1 - X* Math.exp(-intrate*T)*Pd2;

    //A real option value can not be negative
    if(ROV<0) ROV=0;

    String solution = String.valueOf(ROV);
    SolutionTextField.setText(solution);
    }
}
```

Appendix B - AHP Calculator

```
private void Valuation_ButtonActionPerformed(java.awt.event.ActionEvent evt) {
// Value Button
// Matrices (For each objective, 1 for objectives itself) have to be filled with input values

    try{
        if(obj_runner == Objective.Number){fill_Matrix_obj ();return;}

        if(obj_runner==0) {fill_Matrix_1 (); return;}
        if(obj_runner==1) {fill_Matrix_2 (); return;}
        if(obj_runner==2) {fill_Matrix_3 (); return;}
        if(obj_runner==3) {fill_Matrix_4 (); return;}
        if(obj_runner==4) {fill_Matrix_5 (); return;}
    } catch (Exception e)
    {
        getTitles.setText("You_have_done_something_wrong_");
    }

private void fill_Matrix_1 ()
{
    //weighted variable
    double weight_tmp = preferences.getSelectedIndex()+1;

    if(opposite_checkbox.isSelected()==false)
    {
        weight_tmp=1/weight_tmp;
    }

    //set the invers value to the opposite matrix point
    Matrix_1.set(i_run ,j_run ,1/weight_tmp);
    Matrix_1.set(j_run ,i_run ,weight_tmp);

    Matrix_1.print(3,5);

    //Check end of matrix
    if(j_run==Alternative.Number-1 && i_run == Alternative.Number-2)
    {
        obj_runner++;
        i_run=0;
        j_run=1;
        return;
    }

    j_run++;
    //if j-run is at the end of the matrix go to next line
    if(j_run>=Alternative.Number)
    {
        j_run=0;
        i_run++;
    }
    //if we are at the left side of the matrix get on the right side
    while(i_run>=j_run)
    {j_run++;}
}

public void ahp_calculation ()
{
    valuation_text.setText("Calculating...");

    //Normalize Matrix
    double sum=0;
    for (int j = 0; j<Alternative.Number;j++)
    {
        for (int i=0;i<Alternative.Number;i++)
        {
            sum = sum + Matrix_1.get(i ,j);
        }
        for(int i =0;i<Alternative.Number;i++)
        {
            double norm_value = Matrix_1.get(i ,j)/sum;
            Matrix_1.set(i ,j ,norm_value);
        }
        sum=0;
    }

    //Calculate Eigenvector
    for(int i = 0; i<Alternative.Number;i++)
```

```

    {
        for (int j = 0; j<Alternative_Number;j++)
        {
            sum = sum + Matrix_1.get(i, j);
        }
        Solution.set(0, i, sum/Alternative_Number);
        sum=0;
    }
Solution.print(3,5);

//Consistency Check
if(Alternative_Number > 2)
{
    double lambda_max = 0;
    double CI = 0;
    double CR = 0;

    for(int i = 0; i<Alternative_Number;i++)
    {
        lambda_max = lambda_max + (1/Matrix_1.get(i, i)*Solution.get(0, i));
    }
    CI=(lambda_max-Alternative_Number)/(Alternative_Number -1);
    CR=CI/RI[Alternative_Number -1]*100;
}

public void eigenvector_mult()
{
    double mult=0;
    for (int i = 0; i<Objective_Number;i++)
    {
        for (int j=0;j<Alternative_Number;j++)
        {
            mult = vector_obj[i]*Solution.get(i, j);
            Solution.set(i, j, mult);
        }
    }
    Solution.print(3,5);

// Add colums up and save values in vector_sol
double sum = 0;
for (int i = 0; i<Alternative_Number;i++)
{
    for (int j=0;j<Objective_Number;j++)
    {
        sum = sum+Solution.get(j, i);
    }
    vector_sol[i]=sum;
    sum=0;
}

// Do final search for max value
max = 0;
max_index = 0;
for(int i =0; i<Alternative_Number;i++)
{
    if(vector_sol[i]>max)
    {
        max = vector_sol[i];
        max_index=i;
    }
}
return;
}
}

```

Appendix C - MODS Calculator

```

private void Max_Min_ButtonActionPerformed(java.awt.event.ActionEvent evt)
{
    ///Prepare for Complete Enumeration///
    while(Max_Min_Run < Objective_Number)
    {
        // 1 for Maximization
        if(Max_Min_Combo_Box.getSelectedIndex() == 0)
            Max_Min_Array[Max_Min_Run] = 1;
        // -1 for Minimization
        if(Max_Min_Combo_Box.getSelectedIndex() == 1)
            Max_Min_Array[Max_Min_Run] = -1;
        //Get input for next objective
        Max_Min_Run++;
    }

    // create field/vector for variation
    boolean[] portfolio_flags = new boolean[portfolio.size()];

    // set them all false (0)
    for(int i = 0; i < portfolio.size();i++)
    {
        portfolio_flags[i] = false;
    }

    //number of alternatives, to value the length of the field
    double max_index = Math.pow(2, portfolio_flags.length);

    // Put the first alternative in the paretoefficient portfolio
    Pareto_efficient_portfolio.add(portfolio_flags);

    boolean[] transfer = new boolean[portfolio_flags.length];
    for(int i = 0; i < portfolio.size();i++)
    {
        transfer[i] = false;
    }
    //call complete enumeration
    complete_enumeration(transfer, max_index);
}

private void complete_enumeration(boolean[] a, double number_of_iterations)
{
    for(int i = 0; i<number_of_iterations;i++)
    {
        if(a[runner] == false)
        {
            a[runner] = true;
            calculate(a);
        }
        else
        {
            while(a[runner] == true && runner < a.length)
            {
                a[runner]=false;
                runner++;
                if(runner==a.length) runner=0;
            }
            if(runner < a.length)
            {
                a[runner] = true;
                runner=0;
                calculate(a);
            }
        }
    }
}

private void calculate(boolean[] alternative)
{
    int[] alternative_value = new int [Objective_Number];
    alternative_value = get_portfolio_value(alternative);

    //counts in how many objectives proposed alternative is better
    int counter = 0;

    //check if proposed solution is pareto efficient comparing to the previous solution
    //pareto efficient = ALL values have to be better than the others.
    for(int i = 0; i < Pareto_efficient_portfolio.size(); i++)

```

```

{
    //temporary array to store the pareto-effecient-portfolios
    boolean[] tmp = (boolean[]) Pareto_efficient_portfolio.get(i);
    //and get value
    int[] pareto_value = new int[Objective_Number];
    pareto_value = get_portfolio_value(tmp);

    //now compare the real solutions
    for(int j = 0; j<Objective_Number; j++)
    {
        if(pareto_value[j]<alternative_value[j])
        {
            counter++;
        }
    }
    //remove/add pareto efficient portfolios
    if(counter == Objective_Number)
    {
        Pareto_efficient_portfolio.remove(i);
        i--;

        if(i == Pareto_efficient_portfolio.size()-1)
        {
            boolean[] transfer = new boolean[alternative.length];
            for(int z = 0; z < portfolio.size();z++)
            {
                transfer[z] = alternative[z];
            }
            Pareto_efficient_portfolio.add(transfer);
        }
    }
    // if some objectives are better and some are not only add
    if(counter > 0 && counter < Objective_Number)
    {
        if(i == Pareto_efficient_portfolio.size()-1)
        {
            boolean[] transfer = new boolean[alternative.length];
            for(int z = 0; z < portfolio.size();z++)
            {
                transfer[z] = alternative[z];
            }
            Pareto_efficient_portfolio.add(transfer);
            i++;
        }
    }
    counter=0;
}

private int[] get_portfolio_value (boolean[] alternative_selection)
{
    // create arrays for solution values
    int[] solution_values_alternative = new int[Objective_Number];
    int[] temp_values = new int[Objective_Number];

    for(int i = 0; i < portfolio.size(); i++)
    {
        for(int j = 0; j < Objective_Number; j++)
        {
            if(alternative_selection[i])
            {
                //fetch the int[] of portfolio and store it in values
                temp_values = (int[]) portfolio.get(i);

                //Sum them up
                solution_values_alternative[j] = solution_values_alternative[j]+temp_values[j];
            }
        }
    }
    // look if the objective should be minimized or maximized (simply multiply solution by 1 or -1
    for(int i = 0;i<Objective_Number;i++)
    {
        solution_values_alternative[i] = solution_values_alternative[i] * Max_Min_Array[i];
    }
    return solution_values_alternative;
}

//Perform Final Step: Remove pareto efficient portfolios by Min/Max Values
private void caluclate_boundaries()
{

```

```

boolean[] pareto_efficient_alternative = new boolean[portfolio.size()];
int[] solution_values = new int[Objective.Number];

for(int i = 0; i < Pareto_efficient_portfolio.size(); i++)
{
    pareto_efficient_alternative = (boolean[]) Pareto_efficient_portfolio.get(i);
    solution_values = get_portfolio_value(pareto_efficient_alternative);

    for(int j = 0; j < Objective.Number; j++)
    {
        //If its a Minimum Value for Maximization
        if(Boundary_values[j] > solution_values[j] && solution_values[j] > 0 && i >= 0)
        {
            Pareto_efficient_portfolio.remove(i);
            i--;
        }
        //If its a Maximum Value for Minimization
        if(Boundary_values[j]*(-1) > solution_values[j] && solution_values[j] < 0 && i >= 0)
        {
            Pareto_efficient_portfolio.remove(i);
            i--;
        }
    }
}
}

```

Appendix D - MOST Get portfolio value

```
private double[] get_portfolio_value (boolean[] alternative_selection)
{
    // create arrays for solution values
    double[] solution_values_alternative = new double[objectives_array.size()+cost_categories.size()];
    double[] temp_values = new double[objectives_array.size()+cost_categories.size()+1];
    double[] Solution_cost_array = new double[cost_categories.size()];

    double[] VAL_ARRAY = (double[]) VAL_IT_Benefit_array.get(0);
    double[] Risk_ARRAY = (double[]) Risk_ARO_EXF_array.get(0);
    double[] Solution_ARRAY = new double[objectives_array.size()];
    ArrayList tmp_solution = new ArrayList();

    //CALCULATE right PART OF THE FORMULA in order to get the TOTAL ARO FOT IT ALTERNATIVE
    double SUM_ARO = 0;

    for(int i = 0; i < Risk_ARO_EXF_array.size(); i++)
    {
        Risk_ARRAY = (double[]) Risk_ARO_EXF_array.get(i);
        SUM_ARO = Risk_ARRAY[0];
        for(int j = 1; j < Risk_ARRAY.length; j++)
        {
            Solution_ARRAY[j-1] = SUM_ARO*Risk_ARRAY[j];
        }
        //again: why the hack???? it works....
        double[] transfer = new double[objectives_array.size()];

        for(int j = 0; j<objectives_array.size();j++)
        {
            transfer[j] = Solution_ARRAY[j];
        }

        //add in solution array
        tmp_solution.add(transfer);
    }
    //Create AEFF

    // integer array to save indices from eff array
    boolean[] eff_indices = new boolean[Effectiveness_array.size()];

    //counts the number of selected safeguards in portfolio:
    int counter_amount_of_selected_safeguards = 0;

    for(int k = 0; k < alternative_selection.length;k++)
    {
        if(alternative_selection[k])
        {
            for(int z = 0; z < Effectiveness_array.size(); z++)
            {
                String compare_string_selected_Safeguard = (String) safeguards_array.get(k);
                String compare_string_effectivity = (String) EFF_STRING_array.get(z);
                compare_string_effectivity = compare_string_effectivity.substring(0, eff.indexOf(", "));

                if(compare_string_selected_Safeguard.equalsIgnoreCase(compare_string_effectivity))
                {
                    eff_indices[z] = true;
                }
            }
            double[] tmp = (double[]) safeguard_cost_function_array.get(k);
            // Create Solution Cost Array
            for(int z = 0; z < Solution_cost_array.length;z++)
            {
                Solution_cost_array[z] = Solution_cost_array[z]+tmp[z];
            }
            counter_amount_of_selected_safeguards++;
        }
    }
    //At this point I know what eff indices needs to be taken according to the selected safeguards:
    // According to this selection the next step results in the comparison of > 1
    //selected safeguards which reduce both the same vulnerability:

    ArrayList all_indices_safeguards_for_aggregated_effectiveness = new ArrayList();
    for(int i = 0; i < eff_indices.length;i++)
    {
        ArrayList actual_indices_safeguards_for_aggregated_effectiveness = new ArrayList();
        boolean help_counter = true;
    }
}
```

```

for(int j = i+1; j < eff_indices.length;j++)
{
    //get the vulnerability
    String eff_vul_1 = (String) EFF_STRING_array.get(i);
    eff_vul_1 = eff_vul_1.substring(eff_vul_1.indexOf(",")+1,eff_vul_1.length());

    String compare_string_effectivity_vul_2 = (String) EFF_STRING_array.get(j);
    eff_vul_2 = eff_vul_2.substring(eff_vul_2.indexOf(",")+1,eff_vul_2.length());

    if(eff_vul_1.equalsIgnoreCase(eff_vul_2) && eff_indices[i] == true && eff_indices[j] == true)
    {
        //This differentiation is necessary for > 2 safeguards which reduce the same vulnerability
        if(help_counter == false)
        {
            actual_indices_safguards_for_aggregated_effectiveness.add(j);
        }
        if(help_counter)
        {
            actual_indices_safguards_for_aggregated_effectiveness.add(i);
            actual_indices_safguards_for_aggregated_effectiveness.add(j);
            help_counter = false;
        }
    }
}

if(actual_indices_safguards_for_aggregated_effectiveness.size()>0)
{
    int[] transfer_indices = new int[actual_indices_safguards_for_aggregated_effectiveness.size()];
    //store the actual int values in all_indices
    for(int w = 0; w < actual_indices_safguards_for_aggregated_effectiveness.size();w++)
    {
        int safe_tmp = (Integer) actual_indices_safguards_for_aggregated_effectiveness.get(w);
        transfer_indices[w] = safe_tmp;
    }
    all_indices_safguards_for_aggregated_effectiveness.add(transfer_indices);
}
}

//At this point I know all combinations of selected safeguards which reduce the same vulnerability
// which is needed for the aggregated effectiveness
//In the next step compare them associated risks

double[] aggregated_effectiveness = new double[objectives_array.size()];
double[] modified_ARO = new double[objectives_array.size()];

//fill them with 1 (that means that ALE would not change)
for(int i = 0; i < objectives_array.size();i++)
{
    aggregated_effectiveness[i] = 1;
}
//second array for additional values
double[] aggregated_add = new double[objectives_array.size()];

for(int i = 0; i < eff_indices.length;i++)
{
    for(int j = 0; j<Risk_ARO_EXF_array.size();j++)
    {
        if(eff_indices[i])
        {
            eff_vul = (String) EFF_STRING_array.get(i);
            eff_vul = eff_vul.substring(eff_vul.indexOf(",")+1,eff_vul.length());

            risk_vul = (String) risks_array.get(j);
            risk_vul = risk_vul.substring(0,risk_vul.indexOf(","));

            //This comparison is true if the vul of selected eff index equals the vulnerability of risk
            if(compare_string_effectivity_vul.equalsIgnoreCase(compare_string_risk_vul))
            {
                boolean control_flag = false;

                //control if aggregated_effectiveness is needed
                if(all_indices_safguards_for_aggregated_effectiveness.size()>0)
                {
                    for(int k = 0; k < all_indices_safguards_for_aggregated_effectiveness.size();k++)
                    {
                        int[] comparison = (int[]) all_indices_safguards_for_aggregated_effectiveness.get(k);
                        //if the actual index is included calculate the aggregated effectiveness
                        if(i == comparison[0])
                        {
                            control_flag = true;
                        }
                    }
                }
            }
        }
    }
}

```



```

        for(int z = 0; z < comparison.length; z++)
        {
            aggregated_add = (double[]) Effectiveness_array.get(comparison[z]);
            //hardcoded: (for 3 benefit categories)
            aggregated_effectiveness[0] = aggregated_effectiveness[0] * (1-aggregated_add[0]);
            aggregated_effectiveness[1] = aggregated_effectiveness[1] * (1-aggregated_add[1]);
            aggregated_effectiveness[2] = aggregated_effectiveness[2] * (1-aggregated_add[2]);
        }
    }
}

//normal effectiveness because there are not multiple selected safeguards for same vulnerability:
if(control_flag)
{
    double[] Aro_exf_tmp = (double[]) tmp_solution.get(j);

    for(int h = 0; h<Aro_exf_tmp.length; h++)
    {
        Aro_exf_tmp[h] = Aro_exf_tmp[h]* aggregated_effectiveness[h];
    }
    //add modified solution and remove old one
    tmp_solution.add(j, Aro_exf_tmp);
    tmp_solution.remove(j+1);
}
//control sequence for checking if eff index is already included in aggregated effeciny
boolean checking = false;
for(int k = 0; k < all_indices_safeguards_for_aggregated_effectiveness.size(); k++)
{
    int[] comparison = (int[]) all_indices_safeguards_for_aggregated_effectiveness.get(k);

    for(int g = 0; g < comparison.length; g++)
    {
        if(i == comparison[g])
        {
            checking = true;
        }
    }
}
if(control_flag == false && checking == false)
{
    double[] eff_of_safeguard_tmp = (double[]) Effectiveness_array.get(i);
    double[] Aro_exf_tmp = (double[]) tmp_solution.get(j);

    for(int h = 0; h<Aro_exf_tmp.length; h++)
    {
        Aro_exf_tmp[h] = Aro_exf_tmp[h]* (1 - eff_of_safeguard_tmp[h]);
    }
    //add modified solution and remove old one
    tmp_solution.add(j, Aro_exf_tmp);
    tmp_solution.remove(j+1);
}
}
}
}
double[] nearly_solution = new double[objectives_array.size()];

for(int i = 0; i < tmp_solution.size(); i++)
{
    double[] tmp_array_for_tmp_solution = (double[]) tmp_solution.get(i);

    for(int j = 0; j < nearly_solution.length; j++)
    {
        nearly_solution[j] = nearly_solution[j] + tmp_array_for_tmp_solution[j];
    }
}
for(int j=0; j < nearly_solution.length; j++)
{
    nearly_solution[j] = nearly_solution[j] * VALARRAY[j];
}
ALE_Objectives_array_after_Safeguard.add(nearly_solution);
double[] cost_after_safeguard = (double[]) ALE_Objectives_array_after_Safeguard.get(0);

for(int i = 0; i < cost_before_safeguard.length; i++)
{
    solution_values_alternative[i] = cost_after_safeguard[i];
}
// Add cost into the solution Array
solution_values_alternative[0] = solution_values_alternative[0]*-1;

```

```
    solution_values_alternative[1] = solution_values_alternative[1]*-1;
    solution_values_alternative[2] = solution_values_alternative[2]*-1;
    solution_values_alternative[3] = Solution_cost_array[0]*-1;
    solution_values_alternative[4] = Solution_cost_array[1]*-1;

    ALE_Objectives_array_after_Safeguard.remove(0);

    return solution_values_alternative;
}
```