TECHNISCHE UNIVERSITÄT WIEN

VIENNA UNIVERSITY OF TECHNOLOGY

MASTERARBEIT

DEVELOPMENT AND IMPLEMENTATION OF A QUANTITATIVE MULTI-DISCIPLINARY INFORMATION SECURITY RISK ANALYSIS WORKSHOP

July 28, 2006

Ausgeführt am Institut für

Softwaretechnik und interaktive Systeme

der Technischen Universität Wien

unter der Anleitung von:

O. Univ. Prof. Dr. A Min Tjoa

durch

Bakk. Techn. Michael Schramel

Kahlenbergerstraße 55, 1190 Wien

_____ _____

Datum Unterschrift

Abstract

ENGLISH ABSTRACT:

In recent years, incidences of Internet and computer-related crime have risen both in the level of professionalism and fiscal impact. The field of information security management is becoming more and more prominent, evidenced by the large number of new methods and approaches. However, existing approaches to information security management are either very costly (risk analyses) or incomplete and untailored (checklists and best practices). Many focus too heavily on technical solutions, ignoring the social and managerial aspects.

This thesis develops a new approach based on a holistic quantitative risk analysis supported by a group decision support system (GDSS). It explains how information security risks and safeguards can be defined and quantified, how group decisions can be effectively and efficiently made and how alternatives can be ranked. The first stage of the proposed solution is to make clear the requirements for a GDSS for information security risk analyses in groups. Next, a workshop concept is developed, implemented and validated against the requirements based on empirical findings gathered through a case study. The proposed solution enables groups of decision makers to model information security decisions using multiple criteria during a short workshop. It is designed to reduce the risks of group decision-making and to provide an efficient and complete quantitative assessment of group members' preferences. Based on a statistical analysis of the data supported by GDSS portfolio analysis, Pareto optimisation, Monte-Carlo simulation and sensitivity analysis functionalities, efficient safeguards can be quickly identified and recommendations formulated. The present approach, based on quantitative analysis methods, ensures that decision makers are more satisfied with outcomes and that the validity of the decision making process is acceptable on the managerial level.

GERMAN ABSTRACT:

In den letzten Jahren hat Internet und Computer Kriminalität an Professionalität und Einfluss auf Unternehmen zugenommen. Wirksames information security management wird für Unternehmen immer wichtiger, wie die steigende Anzahl an Frameworks und Verfahren beweist. Verfügbare information security management Verfahren sind entweder sehr kostenintensiv (Risiko Analysen) oder unvollständig und nicht Kunden-spezifisch (Check-Listen und Best Practises). Die Mehrheit legt den Schwerpunkt auf technische Lösungen und vernachlässigt die soziale und organisatorische Komponente.

Diese Arbeit stellt ein neues Verfahren vor, das aus einer ganzheitlichen quantitativen Risiko Analyse besteht und durch ein group decision support system (GDSS) unterstützt wird. Sie stellt dar, wie Risiken der Informationssicherheit und Informationssicherheitsmaßnahmen definiert und quantifiziert werden können, wie Gruppenentscheidungen effektiv und effizient erreicht werden und welche Möglichkeiten be-

stehen, Alternativen zu bewerten und zu ordnen. Die Anforderungen (requirements) an ein GDSS, welches Kosten reduzierte Gruppen-Risiko Analysen bei hochqualitativen Ergebnissen ermöglichen soll, werden präsentiert. Anschließend wird ein Workshop Konzept entwickelt, implementiert und anhand der Anforderungen und der empirischen Ergebnisse einer Fallstudie validiert. Die vorgestellte Lösung ermöglicht Gruppen von Entscheidungsträgern, Entscheidungen der Informationssicherheit anhand mehrerer Kriterien im Rahmen eines kurzen Workshops zu modellieren. Es bezweckt die Reduzierung von Risiken, die gehäuft bei Gruppenentscheidungen auftreten, und versucht auf effiziente und komplette Weise, die Präferenzen der Gruppenmitglieder zu ermitteln. Die statistische Analyse der gesammelten Daten - unterstützt durch Funktionalitäten des GDSS wie der Portfolio Analyse, der Pareto Optimierung, der Monte Carlo Simulation und der Sensitivitätsanalyse - ermöglicht die effizienten Sicherheitsmaßnahmen schnell zu identifizieren und Empfehlungen zu formulieren: das vorgestellte Verfahren versucht durch den Einsatz dieser quantitativer Analysemethoden die Zufriedenheit der Entscheidungsträger bezüglich der Ergebnisse zu erreichen und will, dass der Entscheidungsfindungsprozess vom Management angenommen wird.

Acknowledgments

I would like to thank Prof. A Min Tjoa and Thomas Neubauer for their academic support and inspiration. I am particularly grateful for Thomas' endless patience and ambitious ideas, which have made this thesis an equally challenging and rewarding experience. I would also like to thank the uniforce junior enterprise-team that made my case study possible, especially Werner Schmid and Markus Huber, who provided me precious insights into the information security issues of the company. Nathan Ingvalson was so kind to correct my grammar and spelling. Finally I am deeply grateful to my girlfriend Heidi Schrutz, for her wonderful patience and to my parents for their moral support.

Contents

List of abbreviations

ALE Annualized Loss Expectancy

ARO Annualized Rate of Occurrence

BSC Balanced Scorecards

CBA Cost-Benefit Analysis

DSS Decision Support System

GDSS Group Decision Support System

GSS Group Support System

InfoSec Information Security

ISM Information Security Management

IT Information Technology

MADM Multi-Attribute Decision Making

MODM Multi-Objective Decision Making

MOSST (ReMOSST) Multiple Objective (information security) Safeguard Selection Tool

ODIN MODSS The Odin Multiple Objective Decision Support framework

RA Risk Analysis

ROI Return on Investment

ROSI Return on Security Investment

SLE Single Loss Expectancy

1 Introduction

Safeguarding the security of information stored in IT systems is becoming increasingly complex for companies. Limitless information networking technologies are seen as a way to cut costs and to enable new business opportunities. Nevertheless, this environment of continuous innovation combined with the increasing professionalism of computer criminality is accompanied by many new risks which are often difficult to deal with.

1.1 Motivation

Information security measures are often very expensive, while their benefit is often difficult to assess. A complete risk analysis and safeguard selection is very costly and is often replaced by checklists or best practises, the trade-off being resultant solutions that fail to address the specific needs of the organisation and soon become obsolete[1]. A method offering thoroughly analysed results at reasonable costs is missing[2].

Information security is often not viewed as a multi-disciplinary problem which is solely a product of human actions. Currently, in research and in practice, the fact that information security cannot be achieved through technical solutions alone is ignored[3]. Such narrow solutions often fail or prove to be inadequate when implemented in real world situations, leading to over- and/or under-secured assets and high information security related losses. It is therefore necessary to address the issues of completeness in terms of organisational, social and technical solutions[4], which ought to be rated using a complete multiple-criteria set[5].

Moreover, it is important to consider the organisational fit of the information security process and its outcomes. Consequently, information security decisions may be of higher value if made in groups, an idea which has been largely ignored in past literature. As a way to deal with possible group decision shortcomings, group decision support systems (GDSS) have proved to be an adequate means to improve group decision efficiency[6]. Decisions taken by a small group of specialists have often failed to be acceptable to the organisation[7], mainly because of lack of involvement by the organisation's members and the missing organisational match. Groups defined by gdss bring both, leading to better multi-disciplinary decisions

[1] The optimality can be measured in the sum of the ROI (Return of investment) of the security measures implemented.

[2] Stelzer [Ste02, 14].

[3] Finne [Fin00, p. 238].

[4] Zuccato [Zuc02, 16].

[5] Clarke [Cla95, 10].

[6] Mora et al. [MMGAFJNDG02, 52]

[7] See Siponen [Sip00] regarding the importance of motivation for the effectiveness of information security and Darcy [DH04] about a analysis of the factors influencing the effectiveness of information security .

that are acceptable to the members of the organisation. Research about GDSS supported information security risk analysis in multi-disciplinary groups is nonetheless missing[8].

Finally, current research in information security decision making is often based (partly) on qualitative risk analysis models, as adequate data is often missing[9]. Few models exist for the quantitative modeling of information security risks and analysing the model output and the uncertainty of the underlying data[10]. Although models bundling safeguards to portfolios[11] try to provide solutions to these issues, they neglect the uncertainty factor, which leads to incomplete results. Models considering uncertainty are missing.

1.2 Goals

This work presents a GDSS-supported information security risk analysis workshop for groups, which has the benefits of being quantitative and multi-disciplinary while remaining workable and having reasonable budget requirements. For practitioners, it offers a method to quickly and cost-effectively assess what safeguards should be implemented to reduce information security risks[12]. It first needs to address how risks can be modeled quantitatively[13], in order to build a basis on which safeguards will be defined and rated. It then must yield safeguards which can be selected based on multiple criteria, and specify how the uncertainty of the underlying data can be modeled and analysed by sensitivity analysis[14]. Finally the workability of the concept and model are to be put to the test during a case study[15].

For researchers, it presents a new approach for information security risk analyses, based on a multi-disciplinarity, quantification models that permit uncertainty[16], group decision making theory[17] and models[18]. These theories and models must be reviewed and in order to elicit the requirements for a GDSS for information security risk analyses in groups[19]. Finally, a suitable workshop concept, a quantitative risk analysis model and a GDSS will be developed and validated in the course of a case study.

[8] Related research about DSS for information security includes Finne [Fin96c, Fin96b, Fin96a].
[9] Blakley et al. [BMG01, 102].
[10] See [CMBR04, Nic02, SS02, Tan02, Yaz02].
[11] Stummer and Strauss [SS02], Neubauer and Mikscha [NM05].
[12] See 7, 8 and 9.
[13] See 2.
[14] See 8.
[15] See 9.
[16] These include the ALE concept, portfolio management, Monte Carlo simulation and sensitivity analysis.
[17] See 4.
[18] See 5.
[19] See 6

1.3 Structure of this thesis

This thesis presents a method for choosing information security measures in groups and a GDSS-moderated workshop. Two initial chapters 2 cover the field of application: it presents the main characteristics of information security management including the assessment and quantification of risks and security measures. Chapter 5 sketches the pros and cons of decision making in groups in general and relates it back to information security management. In order to limit the drawbacks of working in groups, it is described how group decision systems (GDSS) can assist decision makers in groups and shows in which situations they might be counterproductive. Chapter 7 presents the developed "ReMOSST"-workshop, including a risk assessment workshop, the ReMOSST GDSS and security measure portfolio analysis. Finally, the "ReMOSST"-workshop is presented "in action" and evaluated in chapter 9.

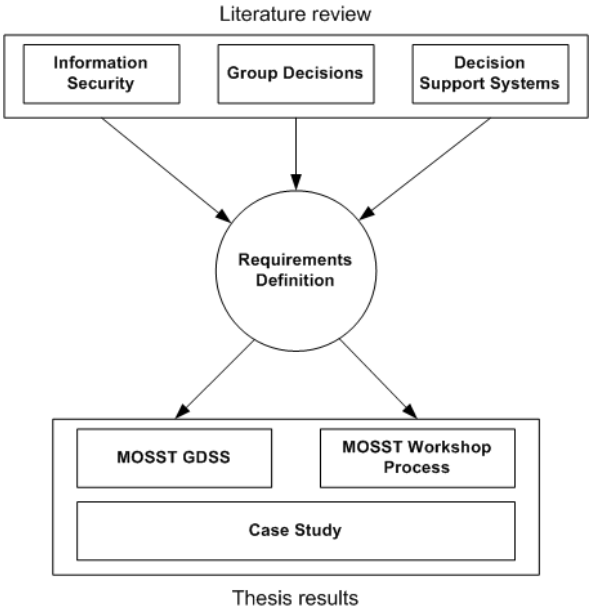


Figure 1: Structure of the thesis

2 An overview of information security management as a discipline

According to the National Information Security Assurance Glossary, information systems security (InfoSec) can be defined as[20]:

[20] NSA [Com03, 33].

> "Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats."

This definition clearly refers to threats on information systems and to security measures. InfoSec and information security management can therefore be seen as related to risk management, as described in sub chapter 2.1. In the following sub chapter 3.1.3, the identification of potential InfoSec goals and their link to the organisation's strategic goals will be described. Finally, the most important factors to consider in InfoSec risk analysis will be defined in sub chapter 2.2.

2.1 Information security management and risk management

Risk management as a discipline deals with risks. The word "risk" is derived from the Italian word "ris(i)care", which can be translated as "to take a chance": this implies that a risk can only be estimated and is never a certainty[21]. Thus, a process for decision making under uncertainty is needed, which is evident in Hoo's [Hoo00, 3] definition of risk management (RM):

> "Risk management is a policy process wherein alternative strategies for dealing with risk are weighted and decisions about acceptable risk are made. The strategies consist of policy options that have varying effects on risks, including the reduction, removal or reallocation of risk. "

Risk analysis (RA) is the process of identifying risks, determining how often they occur and estimating the magnitude of their likely consequences. RA is therefore a method of RM.

Risk management and risk analysis are very similarly defined as information security management (ISM): Finne [Fin98a, 304] even argues that it is an integral part of RM. The "information risk management" framework of KPMG[22] lists security risks as one of eight risk IT RM categories. RM/RA and ISM can be distinguished by their focus: IT RM/RA has a general appeal, i.e. it deals with general IT risks, whereas ISM is solely concerned with InfoSec risks.

Gerber et al. [GvS05] have analysed how risk analysis of RM/RA in general and ISM in particular are related to major science paradigms in order to clarify the relationship between RM and ISM. Figures 2 and 3 summarize the results of their research.

[21] Biffl [BHKS05, 4].
[22] Rauschen [RD04, 22].

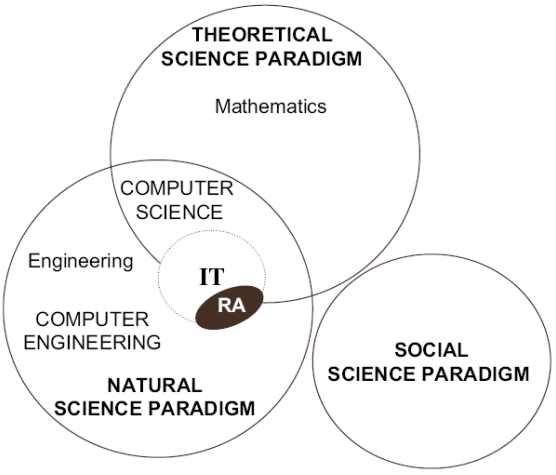


Figure 2: The relationship between risk analysis and major science paradigms (Gerber et al. [GvS05])

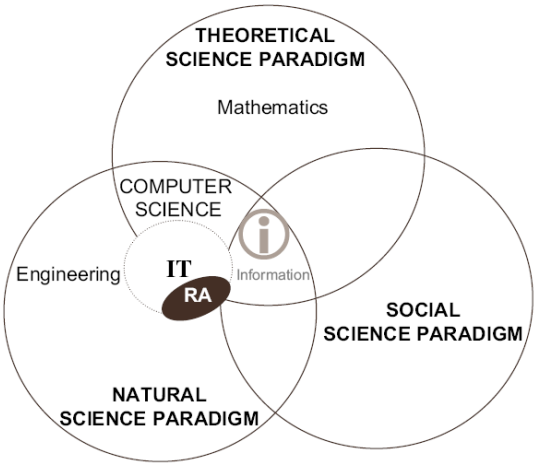


Figure 3: The relationship between *InfoSec* risk analysis and major science paradigms (Gerber et al. [GvS05])

Gerber's [GvS05] main finding is that information is an entity which crosses the borders of the theoretical, social and natural sciences paradigms. Nevertheless information is precisely what ISM is dealing with. Consequently the "classical" IT RA does not suffice for a complete InfoSec RA, as it does not cover aspects of the social science paradigm[23]. In order to be useful for InfoSec purposes it must be extended to "social aspects". This work presents a model which answers explicitly to the specificites of InfoSec risk analysis including the organisational, technical, and social aspects.

[23] This is shown in figure 2.

2.2 The main items of consideration of information security risk analysis

This section provides important definitions of the important items for consideration of information security. Figure 4 provides an overview of these definitions.

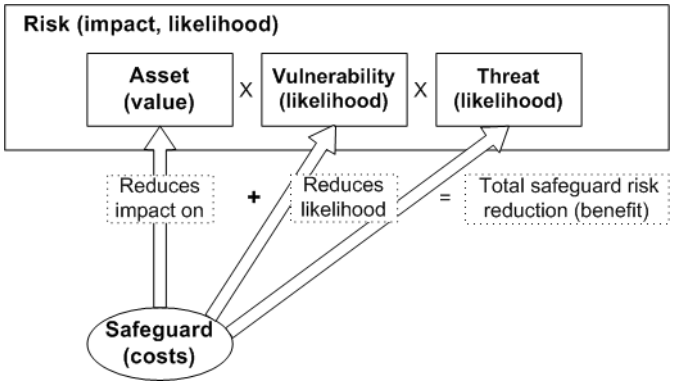


Figure 4: Overview of the main items of consideration in InfoSec risk analysis

Description of figure 4: In general terms, two aspects of information security are of primary importance: *risks* and the *safeguards* designed to cope with these risks. In order to define risks, the questions of what is at risk and against what dangers must be answered by listing all *assets* and *threats*. Additionally, *vulnerabilities* can be explicitly included, as they play a special role in answering the question how bad events can happen. The *cross product* between assets values, vulnerabilities and threats is generally seen as the total set of possible risks[24]. The *impact* of risks can be seen as the effect of risks on asset values in the case of bad events. The likelihood of risks is linked to the likelihood of threats and vulnerabilities. Safeguards are quantified by their costs and their benefits which can be seen in their effect on the impact of risks and the reduction of the likelihood of threats and vulnerabilities.

2.2.1 Asset

An asset can be defined as a element or subsystem of a complex system which information security seeks to protect against threats. According to the official definition of the NSA [Com03, 59], a system asset is:

> "Any software, hardware, data, administrative, physical, communications, or personnel resource within an IS"

[24] Smith [Smi93, 19], in: Finne [Fin98a, 303].

Tan [Tan02, 6-7] differentiates between tangible and intangible assets. Tangible assets are mainly "equipment, hardware and software", intangible assets are typically found in[25]:

- Financial data
- Research & Development research data
- Company reputation
- Sales information
- Marketing research
- Engineering blueprints and specifications
- Trade secrets and know-how
- Computer software

Moreover, one could add business processes and the organisational strategies to the list of intangible assets. The modeling of these items will not be covered by this work for the sake of simplicity.

2.2.2 Vulnerability

The NSA [Com03, 59] defines a vulnerability as a "weakness in an IS, system security procedures, internal controls, or implementation that could be exploited". It therefore can be seen as the "entry point" for a risk to produce an incident. Vulnerabilities that do not pose a threat and do not result in a risk should also be taken into account. The NSA defines these so-called "dangling vulnerabilities" as a:

> "Set of properties about the internal environment for which there is no corresponding threat and, therefore, no implied risk".

2.2.3 Threat

A threat is "any circumstance or event with the potential to adversely impact an IS through unauthorized access, destruction, disclosure, modification of data, and/or denial of service"[26].

Threats do not necessarily result in one or more risks, as they require a vulnerability to be realized. In the case of a threat without an associated vulnerability, one can consider it a

[25] Pavri [Pav99], in: Tan [Tan02, 7].
[26] NSA [Com03].

dangling threat, defined by the NSA [Com03] as:

> "A set of properties about the external environment for which there is no corresponding vulnerability and therefore no implied risk."

According to Bhagyavati et al. [BH03, 250] threats to information security can be categorized as intentional, accidental, active and passive ones:

- **intentional threats:** cause damage to or corruption of the system assets[27].
- **accidental threats:** are due to malfunctions and errors[28].
- **active threats:** change the state of a system[29].
- **passive threats:** do not change the state of the system[30].

This first overview provides an brief insight into the various threats to the security of information systems[31].

2.2.4 Incidents, bad events

According to the NSA [Com03, 59], an information security incident is an "assessed occurrence having actual or potentially adverse effects on an IS". An incident or bad event may be linked to more than one vulnerability and to a set of threats: attacks often rely on multiple vulnerabilities and can potentially pose multiple threats. If incidents are traceable to known vulnerabilities, their rate of occurrence can be estimated and influenced. Nevertheless, if new and unknown vulnerabilities are discovered concurrently with the incident, they must be reported and taken into consideration during the next risk assessment[32].

2.2.5 Risk

A risk - as defined by the NSA [Com03, 59] is:

> "A possibility that a particular threat will adversely impact an IS by exploiting a particular vulnerability"

This definition focuses on the negative impact of InfoSec incidents. Nevertheless, one can easily imagine a situation where risks can have positive effects: for instance, if the Internet

[27] An malicious attack would cause an intentional threat.
[28] A complete taxonomy of malfunctions and errors is provided by Avizienis et al. [ALRL04].
[29] A virus or spy-ware would represent an active threat.
[30] An attacker causing a passive threat might, for example, wiretap the network.
[31] See Farahmand et al. [FNES03] for a complete taxonomy of InfoSec threats.
[32] Blackley et al. [BMG01, 100].

connection of a company fails, employees might be more productive if they are prevented from surfing the Internet for their entertainment. According to Smith [Smi93][33]:

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

Therefore following relation can be defined[34]:

threats + vulnerabilities + asset value = risk

Figure 5: Risk

Nevertheless risks can only be reduced to a certain level, and as a consequence a residual risk has to be taken into consideration:

(threats x vulnerability x asset value) x control gap = residual risk

Figure 6: Residual risk

The likelihood of risks: Based on the likelihood values of vulnerabilities and threats, the probability of a risk can be estimated. This value is often referred to as the *annualized rate of occurrence (ARO),* i.e. the chance that a risk will occur in a year[35].

The impact of risks: Based on the values of the asset at risk, the damages of a bad event can be defined as the impact of the risk. This is often reffered to as the *single loss expectancy (SLE)*[36].

2.2.6 Safeguard

The NSA [Com03, 53] defines safeguards a:

> „A protection included to counteract a known or expected condition.“

This simple definition refers to a „known or expected condition“, i.e. a risk, thus saying that safeguards have the effect of reducing risks[37]. Safeguards affect risks by reducing their

[33] in: Finne [Fin98a].

[34] Smith [Smi93, 19], in: Finne [Fin98a, 303].

[35] e.g. if a risk has a ARO of 0.1%, it is expected to occur once in 10 years. See http://www.riskythinking.com.

[36] e.g. if flooding succeeds in destroying a server computer, the SLE could be estimated using the costs of replacement.

[37] e.g. a firewall reduces the risk of data theft and internet misuse.

impact and their likelihood. Put in the perspective of cost/benefit analysis, safeguard costs and benefits need to be defined.

3 Quantitative information security risk analysis

This chapter presents theories on how to quantify information security risks and safeguards. It begins with an explanation of the organisational prerequisites for a quantitative risk analysis and the areas where it could be implemented. It then describes how items analysed during a RA can be modeled and quantified in 3.2. Finally the aggregation of risks and safeguards and the analysis of the „big picture“ and the modeling of portfolios is discussed in 3.3.

3.1 The information security process and strategy

Information security risk analysis requires a data collection process (Business processes[38], Information systems), followed by a risk analysis (Business processes), then planning the implementation of safeguards (Strategy) and measuring the efficiency (Business processes) of the information security process. These requirements imply that InfoSec needs to be implemented in three areas shown by figure 7: the company's strategy, its processes and obviously its information systems. This section presents the first two aspects and their link to information security.

First, 3.1.1 provides an answer to the question „*Is the organisation ready for an information security process?*“ and presents the Security Maturity Model (SMM)[39]. Second, 3.1.2 describes *which activities of the organisation are covered by a InfoSec process* using Porter's value chain theory[40]. Third, 3.1.3 presents an answer to „*How?*“ by linking strategic goals to InfoSec objectives. Finally, 3.1.4 presents a practical example on *how an InfoSec process can be designed* using the A-SIT methodology[41].

The following figure illustrates which areas will be described in this section:

- **Strategy:** this work argues that information security needs management support and

[38] As defined by „a collection of related structural activities that produce something of value to the organization“, Wikipedia: http://en.wikipedia.org/wiki/Business_process, visited on July 2, 2006.

[39] As described in 3.1.1, this work assumes that an InfoSec process is in place or that the requirements for its implementation are met.

[40] Porter [Por85].

[41] A-SIT [A-S04].

must consider existing strategic goals and associated performance measurement systems in order to be successful[42].

- **Business processes:** developing an information security management process[43] and including it into the other business processes of the company[44] is required to guarantee the continuity and success of InfoSec in the organisation.
- **Information systems:** on the lowest level, InfoSec has to be implemented on the level of information systems. Its success depends directly on the constituent part, including their complexity and the extent to which they are utilised.

In this work, InfoSec safeguards are defined in the contexts of business processes and information systems. InfoSec goals are linked to the strategy level.

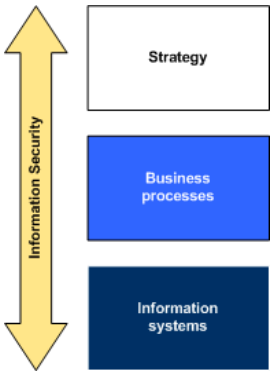


Figure 7: The areas where information security concepts ought to be implemented

3.1.1 The Security Maturity Model and information security process requirements

In analogy to the Capability Maturity Model[45], Thiel [Thi04] defines four steps characterising the maturity of the information security activities in a company, which are shown in figure 8.

Thiel distinguishes four maturity levels among which new improvements are implemented. Each next step is characterised by lower risk and higher costs:

- **Level 0: Blind faith**
  In this level, software remains in the initial configuration, no special security solutions are used and InfoSec safeguards are considered useless and expensive. InfoSec

[42] See 3.1.3.
[43] as described in 3.1.1.
[44] See 3.1.2.
[45] Paulk et al. [PCCW93].

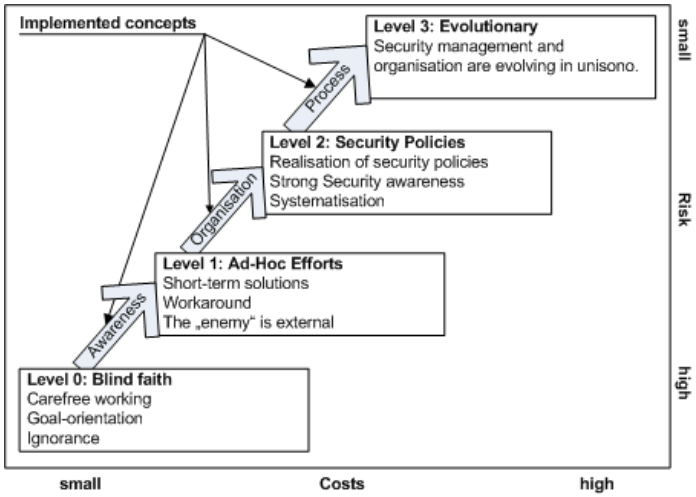


Figure 8: The Security Maturity Model (Thiel [Thi04, 57])

management is not taking place.

- **Level 1: Ad-Hoc efforts**
  This level can be reached through the development of an awareness for information security issues. Nevertheless, incidents trigger ad-hoc efforts, which are not planned systematically: safeguards are implemented, but not regularly maintained. Security breaches are reacted upon, and there is no clearly defined security strategy.

- **Level 2: Policies**
  Through the formulation of security policies, the awareness of the employees rises, the safeguards are kept up-to-date and InfoSec tasks are executed in a professional and systematic way.

- **Level 3: Evolutionary**
  The last maturity step can be reached by implementing InfoSec activities as a process fully embedded in the organisational culture. InfoSec is seen as self-evident and is practiced constantly. All employees are conscious that they are personally responsible for the maintenance of information security; business and security processes are developed together and holistic information security management is capitalised upon as a competitive advantage and an added value for clients.

This maturity model helps one to understand the role of information security in different organisations and the approach required in different contexts. Thus, the ISM process as defined by Thiel [Thi04, 57] can only be implemented if all maturity conditions are fulfilled: high awareness, complete security policies, efficient and state-of-the-art safeguards and extensive know-how.

Nevertheless the final goal of SMM is to reach the last level, which gives employees an

important role in the information security process and requires a holistic approach. For the purposes of this work, a level three organisation with an implemented information security process is to be assumed.

3.1.2 The strategic implementation of the information security process

Information systems play a crucial enabling or improving role in supporting the company's core processes. Information security as a discipline focuses on securing information processed and stored in information systems[46]. By looking at information security as a process embedded in Porter's value chain, its strategic role can be defined more clearly.

Porter states that:

> "The value chain displays total value, and consists of value activities and margin. Value activities are the physically and technologically distinct activities a firm performs. These are the building blocks by which a firm creates a product valuable to its buyers."[47]

Finne [Fin97, 476] describes how information security is to be seen in relationship to Porter's value chain theory. Figure 9 shows the most important support and primary activities of an organisation, which are all relevant for information security, as the examples in Table 1 show:

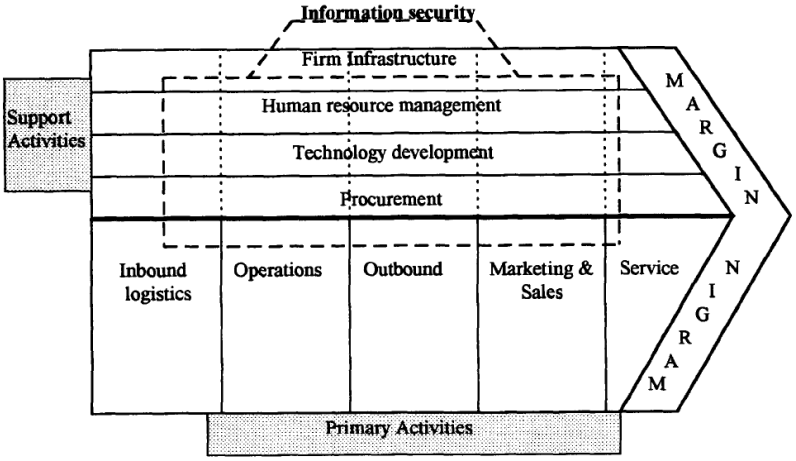


Figure 9: Information security embedded in the value chain (Finne [Fin97, 476])

[46] Solms [SS04b].
[47] Porter [Por85, 38], in: Finne [Fin97, 475].

Activity name:	An example of an InfoSec problem:
SUPPORT ACTIVITIES:	
Firm infrastructure	A strategic plan leaks to the competitor.
Human resources	Disgruntled employees plant viruses.
Technology development	An untested and faulty program is run and causes costs.
Procurement	A unscupulous employee defrauds the company.
PRIMARY ACTIVITIES:	
Inbound logistics	Insecure logistic processes cause information to be stolen.
Operations	A malfunctioning machine causes a power outage.
Outbound logistics	An employee replaces an original product disk with a disc containing a virus.
Marketing and Sales	A drunken salesman tells company secrets to the competitor.
Service	Maintenance though remote access is used by hackers.

Table 1: Porter's value chain activities in the light of InfoSec (Finne [Fin97, 476])

Theses examples show that information security must be considered in all parts of the company and therefore a holistic process to cope with this requirement is necessary. This work chooses an approach that analyses the organisation's processes in order to identify their information security risks and the relevant safeguards required.

3.1.3 How to define information security management objectives

Information security - as a multidisciplinary process - still has to deal with the burden of being considered a purely technical discipline[48]. It is therefore important to define adequate objectives that reflect the multi-disciplinarity of this discipline. This section first presents traditional InfoSec objectives, which have had a strong impact in InfoSec concepts. This is followed by a short description of new concepts of more holistic InfoSec objectives embedded into the strategic view of the organisation.

Traditional information security goals:

Landwehr [Lan01, 6] and Avizienis et al. [ALRL04] list the following traditional security properties information security has to enforce[49]:

- *confidentiality*: assuring that computer-based information is not disclosed without proper authorization

[48] Bjoerck [Bjo01, 87-90].

[49] These three properties are commonly known as the "CIA" properties, see also Atreyi et al. [KTTW03] or Roehrig [Roe03, 26] for a thorough description of these concepts.

- *integrity*: assuring that computer-based information is not modified without proper authorization
- *availability*: assuring that computer-based information is accessible to legitimate users when required

Moreover Landwehr names the following goals which have been recently added[50]:

- *"authentication* (or sometimes identification and authentication): assuring that each principal is who they claim to be
- *non-repudiation*: assuring that a neutral third party can be convinced that a particular transaction or event did (or did not) occur"

According to Finne [Fin98b, Fin00], the CIA concept is limited to small isolated systems. Therefore it does not fit the requirements of modern networked systems which are often directly connected to the Internet and involve varied and numerous users, thus lowering the feasibility of a risk analysis solely based on these criteria.

These traditional concepts of information security have led to a unbalanced focus. According to Blakley [BMG01, 99], "Information security as a discipline is often biased:

- toward technological mechanisms rather than process mechanisms,
- in favor of logical (that is, computer hardware and software) mechanisms, and
- against physical mechanisms (such as locks, walls, cameras, etc...)"

Holistic information security objectives for strategic goals:

Dhillon [Dhi01, 9] states that:

> „Formal models for maintaining the confidentiality, integrity and availability (CIA) of information cannot be applied to commercial organizations on a grand scale“.

Thus, if InfoSec is to be seen as strategic, new objectives and methods have to be found and implemented and traditional models must be put to rest. Dhillon and Torkzadeh[51] describe an array of concrete objectives which clearly show how InfoSec concepts need to be integrated into organisations with the „Overall Objective: Maximize IS Security“:

- Maximize awareness (e.g. create an environment that promotes awareness)
- Maximize data integrity (e.g. minimize unauthorized changes)

[50] See Avizienis et al. [ALRL04] for an a completed taxonomy of dependability and security concepts.
[51] Dhillon and Torkzadeh [DT01, 4], in: [Kol04, p.7].

- Adequate human resource management practices (e.g. provide necessary job resources)
- Maximize organisational integrity (e.g. create an environment of managerial support)
- Developing and sustaining an ethical environment (e.g. develop an understood value system in the organisation)
- Maximize privacy (e.g. emphasize the importance of personal data)
- Enhance the integrity of business processes (e.g. develop understanding of procedures)
- Promote individual work ethics (e.g. minimize the temptation to steal information)
- Enhanced management development practices (e.g. maximize individual comfort level with computers/software)

These objectives are to be reached using intermediate objectives, which assist in forming a favourable environment for InfoSec to succeed. The following examples[52] show which intermediate objectives could improve InfoSec[53]:

- Improve authority structures (e.g. clarify the delegation of authority): supporting the InfoSec goal „Developing and sustaining an ethical environment“
- Ensure empowerment (e.g. promote empowerment in the organisation): supporting the InfoSec goal „Promote individual work ethics“
- Maximize fulfillment of personal needs (e.g. appreciate personal needs for job enhancement): supporting the InfoSec goal „Maximize organisational integrity“

These points show how InfoSec goals can be defined to reflect the overall strategic and operational goals of the company. This helps in ensuring that the focus of InfoSec encompasses all crucial areas. This is highly relevant for this work: first it presents a holistic approach to information security, which attempts to cover all relevant InfoSec aspects. Second it defines management support as a key requirement: it is thus necessary to ensure that the approach chosen is compatible with existing performance measurement systems, which in turn are derived from the organisation's strategic goals.

3.1.4 The information security process in an example

The Austrian Center for Secure Information Technology (A-SIT) has compiled an information security handbook entitled „Österreichisches IT-Sicherheitshandbuch“. This document

[52] More examples can be found in: Dhillon and Torkzadeh [DT01, 4], in: [Kol04, p.7].

[53] Note: these goals are highly relevant for performance measurement instruments like Kaplan and Norton's Balanced Scorecards: see Tewald [Tew04] for the integration of information security objectives into an existing BSC.

is the reference work for eGovernment and eMoney projects in Austria. Its guidelines on how an information security process ought to be set up are adhered to by all public and governmental agencies, including the central bank. This section provides a short overview of this process: it aims to describe how InfoSec processes are set up in real-world organisations in order to define the context for the risk analysis decision making process described in this work is located. An ISM process as defined by A-SIT [A-S04] can be divided into three overlapping phases[54]:

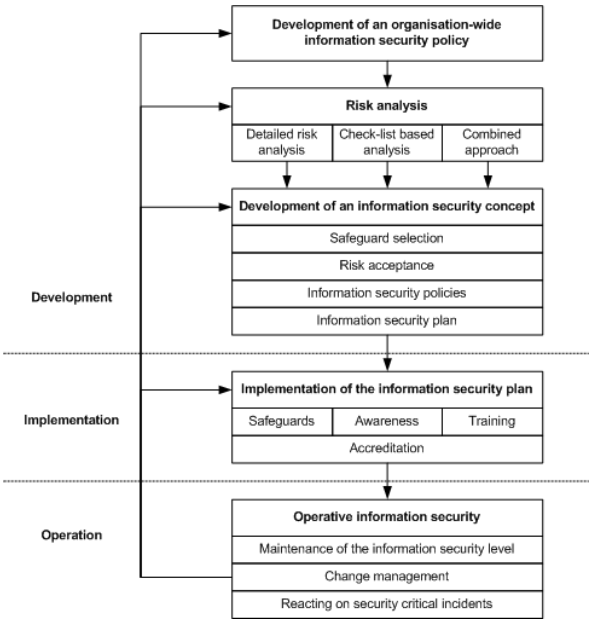


Figure 10: The InfoSec management process according to the A-SIT [A-S04, 11]

Development phase: Definition of information security policies, risk analysis and definition of the ISM concept

This step creates a generic long-term policy covering the InfoSec objectives the organisation intends to reach. This policy is embedded in the overall policies and regulations which apply to this organisation. Additionally, this document can be tailored to the peculiarities of specific organisational units. According to A-SIT [A-S04, 12], the risk analysis can follow three different approaches:

1. A *complete extensive risk analysis* can be executed, targeting the whole organisation.
2. A *check-list approach* yields a basic level of information security at lower costs than for a complete risk analysis
3. A *combined approach* includes a reduced risk analysis which covers the most exposed

[54] A-SIT [A-S04, p.11].

parts of the system, whereas other low-exposure parts can be secured using checklists.

Finally, an InfoSec concept is made up of a short and long term implementation plan with risk acceptance levels, InfoSec measures and policies. This work's risk analysis process is located in this phase and can be defined as a combined approach.

Implementation phase: Implementation of the information security plan

The implementation phase is an essential part of the success of the InfoSec process: the organisational context must be considered with special care. Measures to raise the sensitivity to and the awareness of InfoSec issues assists in the implementation of InfoSec measures and policies. The match between the requirements of the InfoSec plan and the organisational reality has to be ensured.

Operational phase

The operational phase deals with maintaining InfoSec safeguards, checking their conformity to InfoSec policies, reacting to incidents and continuous change management.

3.2 An assessment of the quantifiability of information security

In the context of risk management in the area of information security management, two types of methods have prevailed: on the one side, extensive and costly qualitative or quantitative risk analyses offer company-tailored results - on the other side, checklists and best practices are cheaper formalized means[55] to deal with information security issues, the downside being decision making without a quantitative foundation[56]. The latter uses a "generic structure; derived from a standardized description of IS components and security."[57] The results of both approaches tend to quickly become obsolete after completion of the information security process, they do not allow to specially tailor analyses and their cost gains are often offset by the effort required to keep checklists up-to-date[58]. Moreover, quantification - a important issue for decision making in information security[59] - is not possible with a standardised checklist approach. Even most InfoSec risk analysis models often rely on qualitative ratings, which cannot be easily aggregated to a „bigger picture“, which is crucial for portfolio analysis. The focus of this section is therefore restricted to a description of state-of-the-art quantitative information security management risk analysis concepts[60].

[55] See chapter 3.1 for the Security Maturity Model (SMM).
[56] Stelzer [Ste02, p. 19].
[57] Svenson [Sve05, 6].
[58] Svenson [Sve05, 7].
[59] Dhillon [Dhi01].
[60] Readers interested in checklist approaches could study [A-S04, Bun05].

3.2.1 The quantification of the risk factors

This section presents how the three risk factors, namely assets, vulnerabilities and threats can be quantified in the calculation of the annual loss expectancy of a risk, which in turn is composed of a single loss expectancy (SLE) derived from the asset value times a likelyhood value, or annual rate of occurrence (ARO).

Asset value quantification approaches: The quantification of assets is an essential step in risk analysis. Depending on the approach chosen, the definition of their value varies. Accordingly to Tan [Tan02, 6-7], tangible assets can be valued using their initial capital costs and their depreciation, or alternatively by estimating replacement costs[61]. For intangible assets, the valid methods include the cost, the income and the relief from royalty approach. Moreover, Finne [Fin97, 473] links the value of assets to the point of view of the observer: he argues that assets might have a different value for intruders than for the owner. A few examples how asset values can be defined can be found in Irani [Ira99].

Vulnerability likelihood quantification: Vulnerabilities can be assigned a likelihood of being exploited. Current research focuses on the temporal dimension: as time goes by, the probability of a vulnerability exploit varies, depending on the moment the vulnerability is discovered and at what time it is patched[62].

Threat likelihood quantification: The occurrence of threats can be statistically analysed if appropriate data is available[63] and it is possible to define a likelihood for each threat[64].

3.2.2 Risk impact

As shown in Figure 5, risks are linked to asset values vulnerable should an incident occur. The risk impact can be defined as the values of the asset in danger. An example of a collection of an incident's possible consequences is shown by figure 11. It shows how risk impact can be modeled in detail[65].

[61] Tan [Tan02, 6-7] lists following items to be included in replacement costs: installation costs, troubleshooting costs, loss of business services to customers and employees and 10% contingency.

[62] Arbaugh [AFM00] or Schechter [Sch04, 53-60].

[63] Current reliable data can be downloaded from the websites of the CERT `http://www.cert.org/` and the BSI `http://www.bsi.de`.

[64] Butler [BF02].

[65] For the sake of simplicity, this work models only a single impact value.

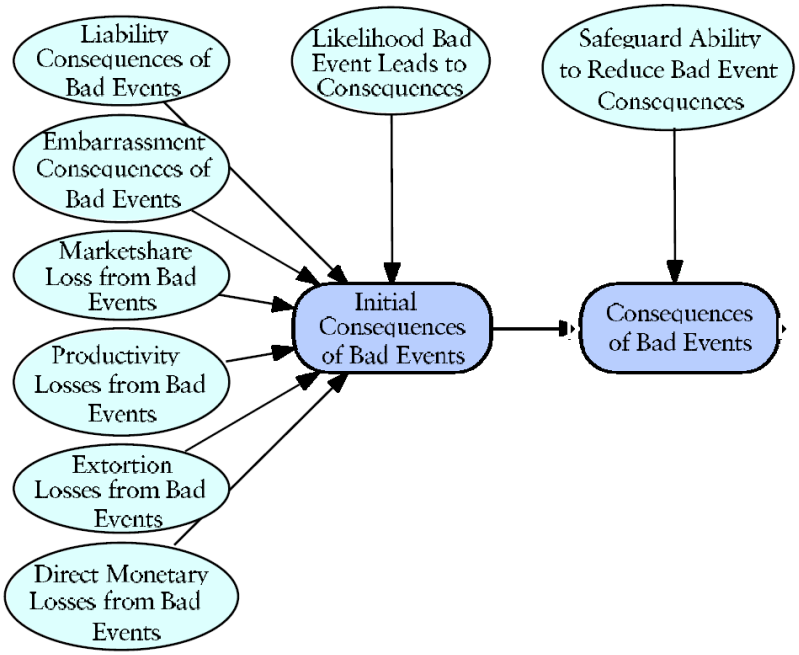


Figure 11: Detailed diagram for consequences of bad events (Hoo [Hoo00, 61])

Hoo describes the sources of uncertainty[66] as follows:

Liability consequences of bad events: If lax computer security in one organization results in damages to others, that organization may be subject to liability lawsuits and be forced to pay damages.

Embarrassment consequences of bad events: Public perception of computer security strength can materially affect the prosperity and success of an organization. To the extent that computer security incidents are publicised, they might cause embarrassment and a damaged reputation.

Marketshare loss from bad events: If a computer security incident results in a loss of intellectual property or a delay in product development or deployment, market share could be lost to competitors.

Productivity losses from bad events: Computer security incidents may reduce employee morale or directly hinder their ability to work, resulting in lower productivity.

Extortion losses from bad events: Because computer security losses could be significant, the possibility exists for malefactors to attempt extortion, threatening harm to an organization unless certain conditions are met.

[66] shown in light blue in figure 11.

Direct monetary losses from bad events: Computer-enabled embezzlement could result in direct monetary losses by an organization.

ALE calculation often uses the figure of a single loss expectancy, which is synonymous with the term „risk impact“ used in this work.

3.2.3 Likelihood of a successful attack

The likelihood of a successful attack is related to multiple factors. The measure used by the ALE concept, the annual rate of occurrence, can be estimated as the quantity of successful attacks during a year's time. Two approaches for estimating this figure can be defined:

The historical data approach:

Figure 12 presents a detailed calculation model by Hoo [Hoo00, 63] to predict the frequency of risks[67].

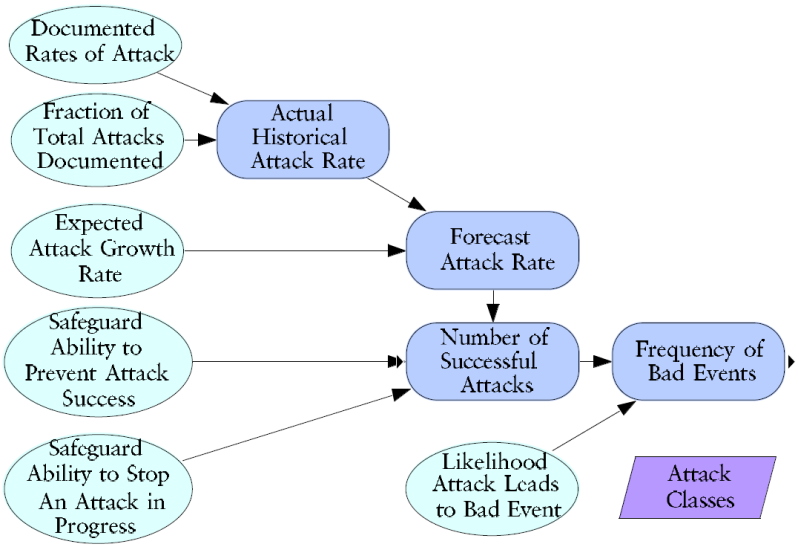


Figure 12: Detailed diagram for frequency of bad events (Hoo [Hoo00, 63])

Hoo describes the sources of uncertainty[68] as follows:

Documented rate of attacks: Historical data on the annual frequencies of different attacks.

Fraction of total attacks documented: Estimate of the attacks reflected in the historical data as a fraction of tha actual number that took place.

[67] For sake of simplicity, this work models only a single frequency value.
[68] shown in light blue in figure 12.

Expected attack growth rate: Expected annual growth in the number of attacks.

Safeguard ability to prevent attack success: Efficacy measure of safeguards' ability to prevent an attack from being successful.

Safeguard ability to stop an attack in progress: Efficacy measure of safeguards' ability to stop an attack in progress.

Likelihood attack leads to bad event: Likelihood that each category of attack will lead to each category of bad event.

This method uses historical data and trend estimations to predict the expected amount of successful attacks. As this kind of data is often unavailable, this approach is seldom practicable.

The vulnerability and threat probability approach:

As an alternative, the likelihood of a successful attack can be estimated by considering the probabilities associated with the risk's vulnerability and threat. Put in context of the risk's asset and its values, these two probabilities are reference-values for the estimation of the risk's likelihood.

Due to the more difficult estimation of a vulnerabilitity's likelihood, this work uses threats' ARO values as reference values for risks.

3.2.4 An assessment of the Annual Loss Expectancy risk metric

A well-known method was developed by the US National Bureau of Standards and was published in 1979 the "Federal Information Processing Standard (FIPS) 65, Guideline for Automatic Data Processing Risk Analysis"[69]: The annual loss expectancy (ALE) is a metric expressing the expected losses linked to a certain risk scenario[70] for one period, usually one year. It can be calculated by multiplying the impact of an incident by its probability:

$$
\begin{aligned}
ALE &= \sum_{i=1}^{n} l(O_i) f_i \\
(O_0, \ldots, O_n) &\quad Set\,of\,harmful\,outcomes \\
l(O_i) &\quad Impact\,of\,outcome\,i\,in\,dollars \\
(f_0, \ldots, f_n) &\quad Frequency\,of\,outcome\,i
\end{aligned}
$$

[69] NIST [NIS02].
[70] Peltier [Pel04].

The following example applies the ALE formula to three possible risks involving bank fraud:

Type of incident	Impact	Frequency	ALE
SWIFT Fraud	$50,000,000	0.005	$250,000
ATM Fraud (large scale)	$250,000	0.2	$50,000
ATM Fraud (small scale)	$20,000	0.5	$10,000

Table 2: Examples of ALE Calculations (Anderson [And01])

The quantification of a risk's ALE still remains a difficult task in InfoSec[71]. Baer [BZ00, 68] enumerates the following major flaws in the ALE concept:

- The frequency of incidents may be subject to the law of large numbers, making estimates are very difficult for most small and medium enterprises.
- Even if the frequency of incidents would be known for a given risk scenario, it still remains difficult to draw conclusions on the effect on the system as a whole[72].
- Risks with very small frequencies and with high impact are bound to be ignored when using ALE calculations to select safeguards.
- The impact estimations are highly dependent on the analysed context. The same incident may cause more or less damage in different organisations.
- Even in middle-sized organisations, the amount of imaginable risk scenarios makes their identification very time-consuming, let alone their ALE calculation.

The ALE concept is therefore very convenient when one wants to find an aggregated value for every risk - under the premise that this figure is understood as a weak estimator. However, it is certainly not an adequate metric for the danger of a given risk: for this purpose, the value of the endangered asset and the expected impact are more appropriate measures.

One can therefore distinguish between two scenarios: first, decision making on the level of single risks needs to consider asset values and impact estimations and be critical of likelihood estimations. Second, decision making in the context of portfolios[73] should make use of ALE aggregations to compare portfolios.

[71] Smith and Spafford [SS04a, p.70].

[72] Blakley et. al [BMG01, 99] highlight that data is often unavailable and that risk factors are often changing, making quantitative calculations prone to errors.

[73] Only critical risks need to be considered in portfolio analysis, as others may be irrelevant and waste important computing ressources and lead to unnecessary complexity.

3.2.5 An assessment of safeguard quantification methods

InfoSec safeguards are - in general terms - proactive or reactive protections against risks threatening an organisation. Before quantifying the efficiency of safeguards, one must first define the roles a safeguard can play. Next, the costs and the efficiency can be estimated.

The multiple roles of safeguards in managing risks

Information security safeguards are controls implemented in order to reduce risks. The relationship between safeguards and risks, defined as the combination of asset values, a threat and a vulnerability is illustrated in figure 13.

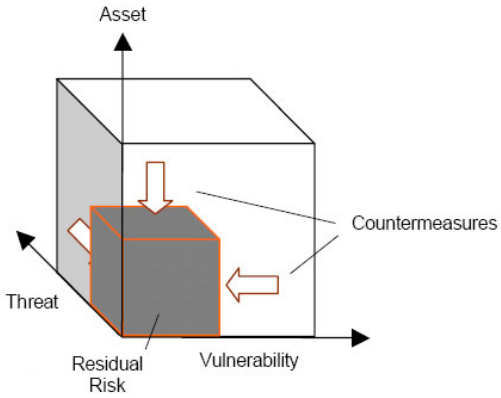


Figure 13: Risk as a function of asset value, threat and vulnerability (Brewer [Bre00], in: Yazar [Yaz02, 3])

Brewer [Bre00] defines values for assets, threats vulnerabilities and safeguards and uses these values to compute a minimal residual risk. Therefore - according to Brewer - safeguards can be of the following types:

- Asset value-reducing safeguards (e.g. back-ups and encryption)
- Vulnerability-reducing safeguards (e.g. procedures, hot-fixes and service packs)
- Threat-reducing safeguards (e.g. firewalls, locked doors, safes and personnel vetting)

For instance, a risk defined as follows could be dealt with through the listed safeguard:

Risk components	Safeguards
Asset: file server	Data encryption with token
Vulnerability: unhindered physical access possible	Locked server room
Threat: data theft and loss of confidentiality	Only store anonymous data

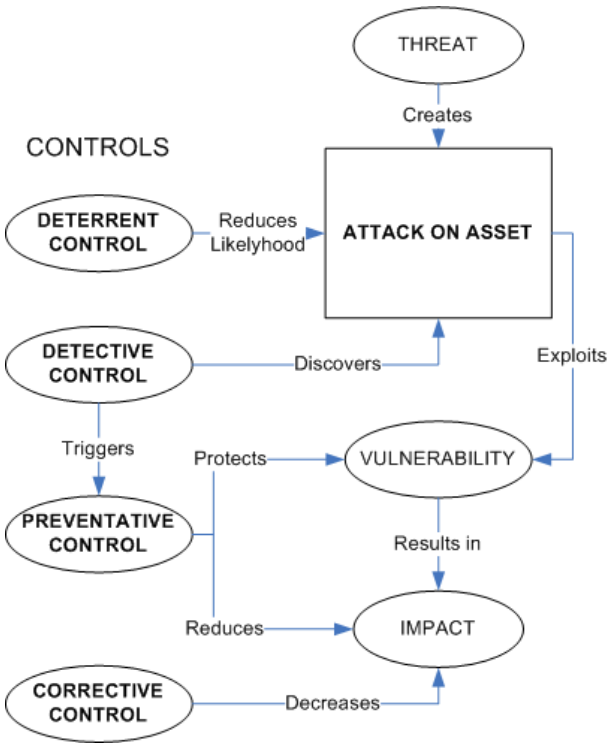


Figure 14: Safety control types according to the COBRA model

As described in the COBRA model, controls can be categorized into the following straightforward types[74]:

- *Deterrent controls*
  An attack, defined as the realisation of a threat reducing the value of an asset, can be deterred by controls: its likelihood decreases accordingly. Therefore, the presence of vulnerabilities is irrelevant for this type of control, moreover it does not influence the impact of a successful attack.

- *Detective controls*
  Detective controls provide ways to notice attacks while they are being executed and enable further controls. In the COBRA model, detective controls do not lower the likelihood of an attack, nor do they reduce its impact.

- *Preventative controls*
  Preventative controls reduce the impact of attacks made possible by a defined set of vulnerabilities.

- *Corrective controls*
  Corrective controls represent the usual course of action when information security

[74] See Figure 14.

safeguards were not able to prevent an attack: the aim is to reduce the damage[75]. For the sake of simplification, one can assume that the reductions in asset value due to damages equal the costs of corrective controls to restore the initial state[76]. Preventative controls enabling corrective controls can be defined so as to make them more efficient in terms of a higher attack impact reduction.

Information security safeguards may be contained in one or more of these categories. For instance, a detective control like an intrusion detection system may deter attackers from hacking a network system, if they are aware that such a system is in place.

The COBRA methodology is very concise on the quantitative relationship of information security safeguards to risks. It is therefore very useful for the development of a quantitative decision support model, which will be described in depth in 3.2.7.

Nevertheless, different perspectives exist covering the subject of safeguard type classification: taken exemplarily, Baer's taxonomy [Bae94] distinguishes between the following qualitative categories to classify information security safeguard properties:

- *Preventive measures* try to stop bad events before they occur: preventive maintenance of hardware certainly reduces risks associated with hardware-related breakdowns and security exposures.
- *Reacting measures* cope with attacks as they occur, e.g. automatic sprinklers and fire extinguishers .
- *Recovering measures* correct the impact of a bad event - appropriated actions have to be taken - for example the recovery of a destroyed database.
- *Risks shifting measures,* for example by procuring insurance covering information security risks, the insurance company takes over the risks.
- *Renouncing*, though disabling services or reducing their functionality, thus lowering risks, for instance by removing access to Internet websites from certain workstations.
- *Ignoring* risks can also be a viable solution if it is done consciously.

Baer's taxonomy defines nearly all approaches to deal with InfoSec risks, except for the detective controls of the COBRA methodology. It explicitly covers other areas COBRA does not even mention: for instance, shifting risks is not an eventuality for the COBRA model. But Baer's classification fails precisely where it excels: it is a qualitative model unfit to analyse the role of safeguards in dealing with risks quantitatively[77].

[75] Therefore, in the best case, assets recover their initial value.

[76] This simplification ignores the fact that down-times can cause further costs, including the opportunity costs of corrective safeguards.

[77] See chapter 3 for a complete taxonomy of InfoSec methods.

For the purpose of this work, the COBRA methodology is the most appropriate, as it allows a quantitative viewpoint of safeguards that is compatible with the quantification concept of Brewer [Bre00].

3.2.6 Safeguard costs

Safeguards can be seen as investments in information security: their goal is to reduce risks. They often result in costs of multiple types. First, *tangible costs* can be named: these include monetary costs, room space, employee work hours, and so on.

Second, modern Cost Benefit Analysis (CBA)[78] often takes *intanglible costs* into account. The idea behind it is to obtain qualitatively and quantitatively better results by modeling variables like key user support by introducing virtual prices: for instance, one can imagine that unpopular spam filters might have high acceptance costs because they may block some legitimate mail. In addition, other important concerns need to be treated appropriately: to name one[79], in modeling ethics costs it would help to include privacy issues in the analysis.

First and foremost, one can conclude that modelling different cost types does make sense, as this is the de-facto standard in modern CBA and as it enables one to include crucial success factors for the implementation of safeguards into the decision making process. Second, depending on the scope of the risk analysis and the subordinate goals[80], different cost types can be defined[81].

3.2.7 Modeling Safeguard effectiveness

The effectiveness of information security measures is highly influenced by a few organisational parameters. Krankanhalli et al. [KTTW03] analyse the role of organisational size, top management support and industry type in its influence on the efficiency of safeguards categorised in „deterrent efforts“, „deterrent severity“ and „preventive efforts“. The results from this empirical study include interesting new perspectives:

- „Deterrent severity (in the form of punishments meted out to IS abusers) does not seem to affect IS security effectiveness.“ Therefore an organisation should focus on user education, policy statements and guidelines (deterrent efforts and preventive efforts).

[78] Murphy [MS01].
[79] A complete list of safeguard costs can be found in Irani [Ira99].
[80] See 3.1.3.
[81] e.g. monetary costs, acceptance costs, cutomer image costs, ethics costs, etc.

- Larger organisations tend to invest more in information security. Krankanhalli et al. argue that smaller organisations need to reassess their level of deterrent efforts, as these correlate strongly with safeguard effectiveness.
- Top management support is of help when preventive safeguards need to be implemented. In order to gain top management support, the authors propose two approaches: first, penetration testing can be carried out, second, the benefit of information security as a way to raise customer confidence can be argued for.
- Depending on the industry type, deterrent efforts and severity vary. Financial organisations, for example, tend to have stiffer deterrents in place. However, Krankanhalli et al. argue that all should focus more on deterrent efforts, as they yield more efficient information security.

D'Arcy and Hovav [DH04] analyse the impact of other variables tied to the potential attacker on the perceived certainty and severity of sanctions:

- High computer self-efficacy - defined as „the individuals' judgment of their computer-related skills in diverse situations" - and high computer experience reduce the perceived certainty and severity of sanctions.
- Age and gender has an effect on the perceived certainty and severity of sanctions: men and younger individuals tend to take more risks, whereas women and older people are more likely to be risk-averse.
- High risk propensity and temporary work contracts moderate the effect of deterrent security countermeasures on both perceived certainty and severity of sanctions.

By considering these variables in risk analysis scenarios, the efficiency of safeguards can be estimated more accurately.

Modeling safeguards and quantifying their relationship toward risks Using the risk quantification methods described above, the effects of safeguards on the annual loss expectancy[82] of a given attack covered in risk R can be modeled as follows:

[82] Hoo [Hoo00, 22].

$$
\begin{aligned}
ALE_1 &= \sum_{i=1}^{n}(F_0(B_i)\cdot D_0(B_i)\cdot \prod_{j=1)}^{m}(1-E_f(B_i,S_j)\cdot I(S_j)) \\
&\quad \cdot(1-E_d(B_i,S_j)\cdot I(S_j))) \\
B_i &\quad Set\,of\,bad\,events\,(incidents) \\
S_i &\quad Set\,of\,safeguards \\
D_i(B_i) &\quad Initial\,estimated\,impact\,of\,bad\,event\,i\,in\,dollars \\
F_i(B_i) &\quad Initial\,estimated\,frequency\,of\,bad\,event\,i \\
E_f(B_i,S_j) &\quad Fractional\,reduction\,in\,frequency\,of\,bad\,event\,i\,as\,a\,result \\
&\quad of\,implementing\,safeguard\,j \\
E_d(B_i,S_j) &\quad Fractional\,reduction\,in\,impact\,of\,bad\,event\,i\,as\,a \\
&\quad result\,of\,implementing\,safeguard\,j \\
I(S_j) &\quad Binary\,function\,indicating\,that\,safeguard\,j\,is\,selected
\end{aligned}
$$

Accordingly, the two types of relationship[83] between a given incident B and a safeguard S can be modeled by a single relative factor f that can be calculated as follows:

$E(B,S) \equiv (1-E_f(B,S))\cdot(1-E_d(B,S))$**,** thus $E(B,S)\in[0,1]$

This equation is visualized in figure 15: The initial ALE risk value, calculated by the product of the impact and the likelihood, is reduced twofold by a safeguard: first, a safeguard reduces the likelihood by the factor $E_f(B,S)$, second it reduces the impact by the factor $E_d(B,S)$. The ALE reduction is shown in gray, the final ALE value after application of the safeguard is shown in white.

[83] A safeguard can affect both a risk's likelihood and its impact.

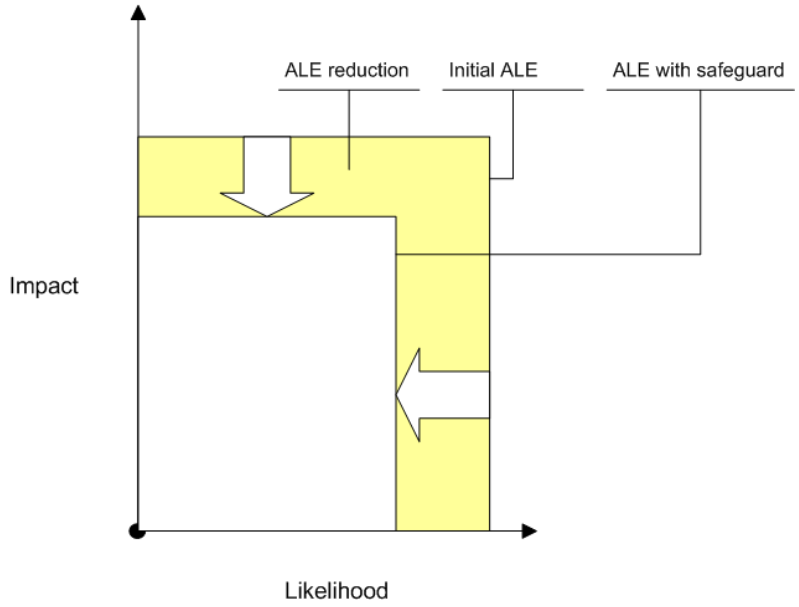


Figure 15: The effect of information security safeguards on the ALE

The cost-benefit of safeguards:

In the case of a safeguard seen as a information security investment, its benefit can be measured by aggregating[84] the ALE reductions and reducing it by its costs[85].

$$
\begin{array}{rcl}
CBR(S) & = & \sum((ALE_0(B) - ALE_1(B)) \cdot I(S,B)) - C(S) \\
CBR(S) & & Cost - Benefit\, of\, safeguard\, S \\
C(S) & & Cost\, of\, safeguard\, S \\
ALE_0(B) & & Initial\, annual\, loss\, expectancy\, of\, bad\, event\, B \\
ALE_1(B) & & Annual\, loss\, expectancy\, of\, bad\, event\, B\, after\, application\, of\, safeguard\, S \\
I(S,B) & & Binary\, function\, indicating\, that\, safeguard\, B\, has\, an\, effect\, on\, bad\, event\, B
\end{array}
$$

For the purpose of this work, this formula will not be used, as efficiency is analysed on the level of portfolios of safeguards. Moreover, costs and ALE values are measured in different units and are not aggregated, as it would be necessary for a cost/benefit calculation.

[84] In this calculation a sum is used to aggregate ALE values.

[85] inspired from Urban [Urb02], in: Tan [Tan02, 6].

3.3 Aggregating risk analysis results: portfolio management

A financial portfolio can be defined as a "collection of assets and collection of prospects"[86]. The goal is to combine assets with different risk profiles in order to lower the overall risk. Proceeding by analogy, as InfoSec safeguards are optional investments, an InfoSec portfolio would be a collection of information security safeguards, selected in the context of a given system with specified risks. Its aim is to reduce the overall risk emanating from information security threats.

Seen trough the perspective of technology management, portfolio management appears as a tool helping to model understandably the „big picture“ of technology endeveours, thus bringing the business and IT worlds[87] together:

> „Portfolio management helps overcome the disconnect in communications between the business and IT communities. It is an excellent way to deal with the perennial questions about IT value and IT alignment with the business.“ Bill Rosser, Gartner

In line with this view of portfolio management, this work suggests an approach that encourages experts and managers to make decisions together by sharing their respective viewpoints.

This section presents how InfoSec portfolios can help reducing the overall InfoSec risk and safeguard costs leading to an optimum level. It also presents how risk analysis results can be aggregated quantitatively to portfolio values, making comparisons between portfolios possible. Finally it discusses how portfolios can be compared when multiple criteria are to be considered by introducing the criteria of Pareto-optimality for information security portfolios.

Portfolio optimality:

Finne [Fin98a, p.4] argues that an optimum level of information security can be achieved. Raising the InfoSec level by spending more on safeguards should result in lower losses, because of a decrease in information security incidents. Therefore, the sum of costs and losses reaches a minimum at a certain information security level, shown in figure 16. In theory, an organisation should try to reach this optimum, as it would then have the best return on investment (ROI) from security measures. Nevertheless, a company might be willing to pay a premium to reach a higher information security level, if it hopes to obtain a competitive advantage, i.e. one that appears convincing to customers[88].

[86] Finne [Fin97, p. 473].
[87] IT Governance Institute [IT 04].
[88] Banks and insurance companies tend to be more risk-averse.

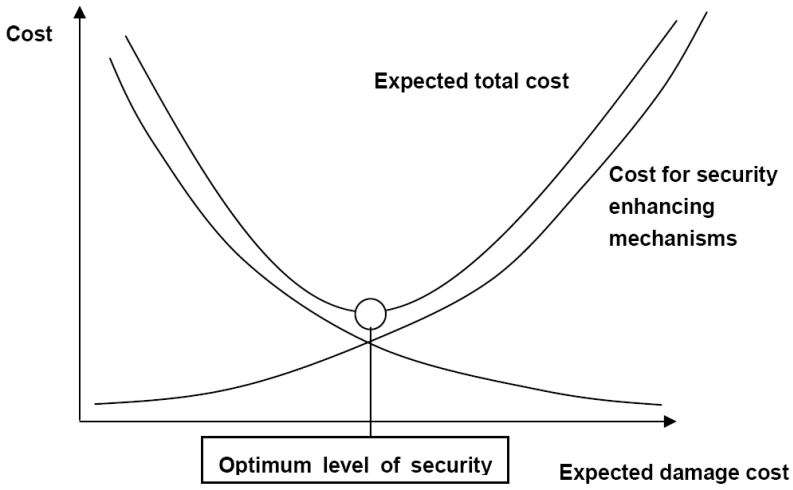


Figure 16: Costs, economic losses, level of InfoSec and optimum (Svensson [Sve05, 8])

Finne's model does not take into account the fact that implementing information security measures can result in externalities: for instance if a Internet service provider (ISP) implements a virus scanner and spam filter for all of its clients, the total benefit[89] to all concerned parties widely surpasses the internal savings of the ISP. Finne's model is therefore limited to small and medium sized organisations, which can implement safeguards without noticeable externalities.

Aggregation of values in portfolios: In terms of safeguards, aggregation can sometimes be impossible: some systems might not be compatible to each other. Moreover, a group of safeguards could yield (dis-)economies of scale if present in a portfolio: for instance, if a firewall is implemented together with a intrusion detection system from the same company, a discount might be applied. Additionally, due to similar operations involved in the installation of the two products, total implementation time could be lowered.

In terms of risks' aggregation, the simple approach of summing the ALE of individual risks into a single aggregated portfolio ALE value might prove inaccurate. Risks might be correlated and causally linked to each other[90]: both their likelihood and their impact can therefore depend on each other. For the sake of simplicity, this work considers each risk as completely independent.

Some possible aggregation methods for uncorrelated cost and ALE values are[91]:

- Linear compensatory decision rule: $x_1 + x_2 + ... + x_n$

[89] The benefit of InfoSec safeguards can be measured by the reduced losses related to risks and incidents.
[90] i.e. a successful attack results in further attacks.
[91] Tompkins [Tom03, 8].

- Cumulative decision rule: $x_1 * x_2 * ... * x_n$
- Polynomial decision rule: $2^{x_1} + 2^{x_2} + ... + 2^{x_n}$

Given the following sample safeguard costs and four-safeguard portfolios, both rules can be applied as follows:

Portfolio	Safeguard cost	Lin. comp. dec. rule	Cum. dec. rule	Poly. dec. rule
p1	1;2;6;0.5	$1 + 2 + 6 + 0.5 = \mathbf{9.5}$	$1 * 2 * 6 * 0.5 = 6$	$2^1 + 2^2 + 2^6 + 2^{0.5} = \mathbf{13.19}$
p2	3.2;4;1.1;2	$3.2 + 4 + 1.1 + 2 = 9.3$	$3.2 * 4 * 1.1 * 2 = \mathbf{28.16}$	$2^{3.2} + 2^4 + 2^{1.1} + 2^2 = 12.19$

Finne [Fin98b, 400] states that due to the lack of historical InfoSec data, risk likelihoods cannot be estimated, making the aggregation of a risk's ALE values difficult. He presents methods that do not require the weighting of possible outcomes, including the following[92]:

- **The Laplace criterion:** Assuming that all outcomes O_i are all equally likely ($p(O_i) = 1/n$ where $i = 1, 2, ..., n$), the alternative A_j with the best expected value $E(A_j)$ is chosen. The Laplace criterion is often inefficient, because of the assumption that outcomes are uniformly distributed.
- **The Minimax (maximin) criterion:** The alternative which scores best in the worst case scenario is chosen. This criterion is highly risk averse, as it focuses uniquely on the (perhaps unlikely) worst case. Risk-seeking decision makers will find this approach inappropriate.
- **The Savage Minimax Regret criterion:** First, the best alternative for each possible case is determined. Second, the distance between each alternative and the best one is computed for each case. Third, the alternative with the lowest maximal distance is chosen. This approach tends to lead to an alternative with less benefit but also less costs.
- **The Hurwitz criterion:** First, weighting factors for the best and worse case are defined. Next, a weighted mean is calculated: the alternative with the best weighted mean is chosen. However, due to the lack of InfoSec data for the weighting of factors, Finne considers this approach not suitable for InfoSec.

For the sake of simplification, this work aggregates values of the same unit[93] using the linear compensatory decision rule[94] and the very similar arithmetic mean. The aggregation of group ratings in DSS bears certain flaws that are described in 4.2[95]. Finally, multi-attribute values[96] for a single item are not aggregated and are compared through Pareto analysis, as

[92] See [Fin98b, 400] for complete descriptions and examples in which these criterion are used for InfoSec decisions.

[93] i.e. cost and value categories.

[94] e.g. a portfolio with three safeguards costing 200, 500 and 1300 EUR will have monetary costs amounting to $200 + 500 + 1300 = 2100$ EUR.

[95] See Tompkins [Tom03, 13] for a critical view of the complexity of GDSS and its reduction in accuracy.

[96] i.e. with different units, e.g.: EUR, image points.

described below.

The Pareto criterion for portfolio optimality

Pareto-optimality is a central theory in economics which measures the economic efficiency and income distribution. It states that a system is optimal according to the Pareto criterion, if it is impossible to favor one individual without harming another.

In the case of multi-criterion InfoSec decision problems and portfolio selection, a portfolio is Pareto-optimal when no other superior[97] one can be found[98].

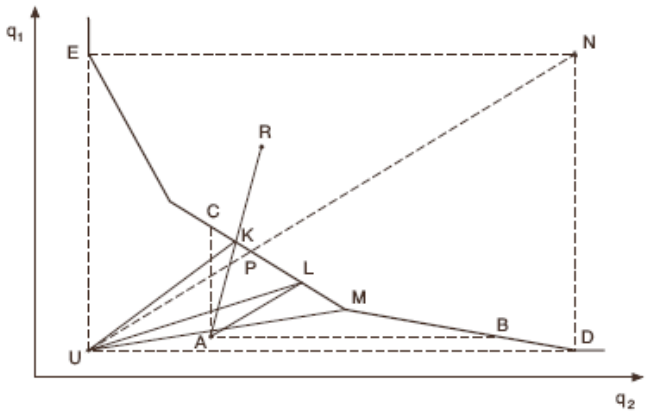


Figure 17: Illustration of a Pareto-optimal surface, and of various selections of efficient solutions for a two-criteria case.

Figure 17 shows an examples of Pareto-efficient solutions in a two criteria case:

- q_1 :First criteria
- q_2 :Second criteria
- Curve E-D: This curve is Pareto-optimal frontier composed of all Pareto-optimal solutions
- Point N: The Nadir point is "composed of the worst values (from the Pareto-set) of all criteria."
- Point U: The Utopia point is defined as the inverse of the Nadir point: it is composed of the best values of all criteria.
- Point R: The "Reservation level" is defined as the minimal values the decision maker is ready to accept.

[97] A portfolio is superior if at least one criterion is "better" and all others are "equal".
[98] Makowski [Mak04, 16].

- Point A: The "aspiration level" is composed of the values the decision maker would like to achieve.
- Point P: This point represents the compromise between Nadir and Utopia points, it is often chosen at the start of the analysis by setting the aspiration and reservation levels to the Nadir and the Utopia points.
- Point K: This point is the compromise between aspiration and reservation levels.

Makowski [Mak04, 17] defines a achievement scalarizing function, which rates Pareto-optimal portfolios and helps to select a given portfolio[99]:

$$\begin{aligned}
\sigma(q, \bar{q}, \bar{\bar{q}}) &= \min_{1 \leq i \leq k} \sigma_i(q_i, \bar{q}_i, \bar{\bar{q}}_i) + \varepsilon \sum_{i=0}^{k} \sigma_i(q_i, \bar{q}_i, \bar{\bar{q}}_i) \\
q & \quad vectors\, of\, values\, of\, criteria \\
\bar{q} & \quad vectors\, of\, values\, of\, aspiration\, levels \\
\bar{\bar{q}} & \quad vectors\, of\, values\, of\, reservation\, levels \\
\varepsilon & \quad given\, small\, positive\, number \\
\sigma_i(q_i, \bar{q}_i, \bar{\bar{q}}_i) & \quad strictly\, concave\, functions\, of\, the\, criteria\, vector\, components\, q_i
\end{aligned}$$

The partial achievement function $\sigma_i(q_i, \bar{q}_i, \bar{\bar{q}}_i)$ can be chosen in order to select portfolios according to different parameters, an example of such parameters would be:

$$\begin{aligned}
\sigma_i(q_i^U, \cdot) &= 1 + \bar{\beta} \\
\sigma_i(\bar{q}_i, \cdot) &= 1 \\
\sigma_i(\bar{\bar{q}}_i, \cdot) &= 0 \\
\sigma_i(q_i^N, \cdot) &= -\bar{\eta}
\end{aligned}$$

Maximizing this function provides a solution with a smaller trade-off coefficient smaller than $1 + \frac{1}{\varepsilon}$. According to Makowski, the parameters $\bar{\beta}$ and $\bar{\eta}$ are typically set to 0.1 and 10, but should be dynamically changed when aspiration and reservation levels are near to Nadir and Utopia points.

Makowski's algorithm uses a formula to compute a ranking of Pareto-optimal portfolios, and is thus an aggregation function between the various criteria. If implemented using software, optimal portfolios can be automatically selected if the variables described above have

[99] In figure 17, points B, M, L K and C are obtained by varying the parameters of this function.

been defined. If not, this algorithm provides guidance on how to deal with multiple-criteria problems and which variables can be manipulated in order to get an optimal portfolio.

3.4 Summary

This section discusses how alternatives that are considered during InfoSec RA can be quantified. In a classical RA setting, it shows how the value of assets can be defined, how the impact value and occurrence rate of risks can be estimated. This provides the base for the definition of InfoSec safeguards, which need to be quantified using three dimensions: their costs, their effect on risks impact, and their effect on risks occurrence rate. Using this data, portfolios of safeguards can be defined: by aggregation each portfolio can be assigned safeguard costs and benefit values, thus making them comparable. Additionally the modeling of dependencies between safeguards is discussed, enabling one to include exclusions, groups and (dis-)economies of scale in the calculations.

Finally the hypothesis of optimality in portfolio calculations is elicited. It states that adding the cost-functions of risks and safeguards, an optimal level of InfoSec expenditure can be calculated.

The presented quantification models are partly implemented by the ReMOSST model described in 8.

4 An evaluation of group decision workshops in information security

Group decision making "involves two or more participants engaged in both decision making and communication"[100]. Group decisions have played an important role in many decision making processes in security-related areas. For instance, the Delphi method[101], one of the most renowned method in this domain, was developed by the Rand Corporation to analyze the risks of nuclear attacks by the Soviet Union.

Current standard methods for group decision workshops in information security are provided by Urban [Urb02]:

Expert interviews: Expert interviews help to gather the data required for an informed decision making process. Alternatively a (semi-)structured questionnaire can be used to support the interview.

Wide-band Delphi technique: A coordinator formulates a problem and provides a scale to experts. The experts rate the alternatives independently and secretly using the given scale. The coordinator combines the results.

Brainstorming: A brainstorming session is a creativity technique. It is structured in two steps: first, group members are invited to name ideas without inhibitions and taking inspiration from other ideas. Next, these ideas are structured and rated.

Nominal group technique: The members of a small group (6-12) write the most important issues down and read them out loud one after the other. The items are written on a pad. Finally, these items are ranked on a final list.

Affinity diagram: The affinity diagram structures brainstorming results into clusters, helping to define the problem area.

Analogy techniques: This techniques links the studied problem to other ideas or things that work similarly. This could provide new insights into the initial problem area.

These widely used techniques are very useful for simple decision making models. In the case of a complex quantitative risk analysis model as described in this work, these methods are inefficient and inadequate because of their unspecific approaches. This work presents a model and workshop concept specially tailored to the intricacies of information security decision making.

This chapter will first present the value of group decisions in information security as a multi-disciplinary field, presented in 4.1. In 4.2 the trade-offs regarding the efficiency and the quality of decision making in groups will be clarified.

[100] Kersten 1997, in: Mustajoki [Mus99, 18].
[101] Linstone and Turoff [HALMT75].

4.1 Group decision workshops for high-quality, multi-disciplinary information security decisions

Inviting stakeholders and key users with different backgrounds to participate in the decision making workshop can yield an increase in the quality of decisions made: the heterogeneity of the group ensures that more information and intelligence is available than it would be the case when only one person would take the same decisions[102]. Embedding representatives of different user groups helps in ensuring a "democratic" decision making workshop, the group mimics the workings of a parliament in today's governments - with all of the advantages and drawbacks. This becomes increasingly important as risks are correlated with the individual's behaviour and implementing information security measures requires the cooperation of every single member of the organisation.

Accordingly, Information Security is a multi-disciplinary field involving many different factors, which widely exceed its traditionally narrow technical scope and give heterogeneous groups of specialists a unique advantage. Zuccato [Zuc02, 16] presents three simplified dimensions[103] covering all major aspects of ISM:

- *The business dimension:* including organisation (partly), legislation (partly), strategy, policy and insurance
- *The social dimension:* including organisation (partly), legislation (partly), awareness and ethics
- *The technical dimension:* including monitoring, evaluating, best practices and certification

In the context of a risk analysis as a key element of a InfoSec process, the required holistic approach must involve a heterogeneous set of stakeholders with the required knowledge and disciplinary background: information security risk analysis ought to bring these stakeholders together.

Moreover, the perceived role of information might vary within the organisation. White and Dhillon [WD05, p. 5] differentiate between four core design ideals which summarize the stakeholders' basic mindsets that influence their conception of information security.

[102] Kersten [Ker97], in: Mustajoki [Mus99, 18].
[103] adapted from Solms [vS01].

- **Private enterprise:** InfoSec and information systems are means to reach certain predefined objectives and should be efficient and reliable.
- **Stattist:** Security and information systems should strengthen institutions, quality has to be reached by opposing conflicting and negotiating point of views.
- **Libertian:** Information security has to support the emancipation of humans so as to realize their full potential. External (power) and internal (psycho-pathological) barriers have to be removed.
- **Neopopulist ideal:** Information security should be intelligible to all stakeholders. Therefore it is important that security designs are not imposed and are based on the organisational context.

According to White and Dhillon, considering these core design ideals in the development process can avoid "any development conflicts resulting in a security compromise" and "the information system will be more effective in its environment as a socio-technical system"[104]. Letting a group make InfoSec decisions makes it easier to find a compromise between the conflicting core design ideals, which could yield qualitatively and quantitatively better results.

Finally, including key users of the information system(s) and stakeholders of the relevant business processes can have the beneficial effect of higher acceptance of the InfoSec processes' results. Additionally, higher awareness can be expected and the efficiency of the InfoSec process raised[105]. According to Rudiger et al. [REHN99, 89-93], three strategies can be combined in order to enhance the effect of information security measures through psychological means:

- **Reduction of the effective security risk:** obviously, showing that security measures effectively reduce risks is helpful: measuring the effect of safeguards is a crucial aspect of ISM.

- **Increase in the knowledge about the (technical) object:** providing users with information about the general and current state of the security of their information systems and business processes reduces uncertainty about InfoSec risks and leads to higher safeguard effectiveness through higher awareness and better application of InfoSec measures[106].

- **Increase in the perceived control over the (technical) object:** providing users means to influence the behaviour of the (technical) object makes him/her accountable and more aware of the importance of security[107].

[104] White and Dhillon [WD05, 5].

[105] Siponen [Sip00].

[106] e.g. showing a warning sign on mobile devices informing the user that he is using weakly secured communication channels raises his/her awareness and deters him/her from transferring sensitive data in such situations.

[107] e.g. people tend to underestimate the risk of a car accident and often overestimate the risk of a plane crash:

Combining these strategies reduces risks directly by affecting the level of threats and vulnerabilities. Indirectly, risks can be reduced by increasing the responsibility of users: acting appropriately, they can be told that risks are reduced, how to identify them and how to act upon them.

4.2 The efficiency and quality issues of group decisions

As shown in the previous section, group decisions can offer certain advantages over decisions taken by a single individual in the context of information security. However, group decision making sometimes may distort the perception of the group members and may lead to suboptimal decisions. This section presents the main flaws or risks involved in group decision making which should be taken into consideration while planning and executing the decision making process.

4.2.1 Decision making in groups and its flaws

Group decisions often fail to yield the expected results. Kersten[108] argues that group decisions are sometimes time-consuming. Moreover, whereas single decision makers already have to deal with the issue of conflicting internal goals, groups will have to handle the lack of knowledge of the other group member goals. Additionally, indecisiveness inside the group may lead to compromises that are "poor to everyone".

Martirossian [Mar01, 19ff] presents the following diverse aspects of group decision making:

- *Group polarisation* often occurs, leading to lower or higher risks; e.g. a group member entering a discussion with a certain viewpoint on risks and the safeguards to implement only becomes more convinced of his opinion after the meeting.
- Often, group decisions tend to rely to heavily on past bad investment decisions, and thus often choose to stick to their initial plans. Martirossian qualifies this as the *"too much invested to quit"-phenomenon*; e.g. an inefficient, difficult to configure spam filter which is refusing legitimate mail was very costly and time-consuming to implement: nobody wants to turn it off and efforts are decided to tweak its behaviour, even though everybody is aware that the efforts are in vain.
- A group member can often impressively shift the group's prevailing viewpoint just by providing a bit of information. This informational influence can be inserted using *expert opinions, statistical information or simply strong arguments;* e.g. the InfoSec

whereas the former are perceived to be easily controlled, the latter are often associated with a strong feeling of helplessness.

[108] Kersten 1997, Mustajoki [Mus99, 18].

experts brings reports that support his proposal for a certain safeguard, which is decided by the group even though other more efficient alternatives exist to cope with this problem.

- By conforming to a certain shared opinion, group members form a norm which lead them to *overvaluing this viewpoint* and to being affected by *normative influence*; e.g. group members tell each other about their bad experiences with e-mail security and give this matter more and more importance, leading to higher risk estimates.

If these items remain unaddressed, group decisions threaten to become unproductive and yield bad results that do not reflect the group's opinion and might therefore be inferior to decisions taken by a single decision maker.

4.2.2 The influence of group parameters in its decision making ability

The group's size, structure, cohesion, leadership and its method for addressing unanimity and majority issues have a strong impact on how a group performs in making decisions effectively and efficiently.

Group size: The size of groups can be an important factor in group decision making as it influences two major performance criteria: larger groups increase the need for communication but limit the time an individual can express himself[109]. This is highly relevant for information security, as InfoSec group decision making only yields the expected benefits if the management, technical experts and representatives of key user groups all participate.

Group structure and cohesion: Two types of groups can be found: homogeneous groups, composed of people with similar backgrounds, and heterogeneous groups with "disparate and dissimilar backgrounds"[110]. Homogeneous groups tend to perform better at executing well defined tasks, heterogeneous are better at problem solving, "broadening the members' horizons and enlivening the interpersonal interactions". Martirossian notes that the latter will tend to turn outwards, thus interacting with outsiders. This is especially relevant for information security for two reasons: one, InfoSec risk analysis requires knowledge of specialists, two, InfoSec decisions are implemented in an organisation. This implies that members of the decision making group should interact with the company's employees, in order to ensure a high acceptance level and the feasibility of decided security measures.

[109] Martirossian [Mar01, 11].
[110] Martirossian [Mar01, 13].

Group leadership: Martirossian [Mar01, 13-15] identified two leadership styles: people-oriented and task-oriented leaders. In summary[111], the former succeed in satisfying the group, though it is not always productive. The latter ensures productivity: group cohesiveness and satisfaction are only reached when "members know what to expect". Due to the complexity of the ReMOSST risk analysis, participants need to prepare adequately before attending a workshop, as it can only be successful with highly productive group work[112].

Group unanimity, compromise and majority: Noorderhaven [Noo98][113] argues that group decisions must be divided in terms of how the decision is reached: A *strictly unanimous decision* is reached when "every group member has to agree that the decision made is the optimal choice". A *consensus* is possible, when "every group member is able to accept the decision on the basis of logic and feasibility". Finally, a *majority* can be achieved if most but not every group member is satisfied with the outcome of the decision making process.

4.2.3 The "groupthink" phenomenon

Martirossian [Mar01] states that group decisions often fail because of the phenomenon of "groupthink", first described by Janis [Jan72]:

> "a quick and easy way to refer to a mode of thinking that people engage in when they are deeply involved in a cohesive in-group, when the members' striving for unanimity override their motivation to realistically appraise alternative course of action."

These phenomenon can be observed when certain structural conditions are met or when the group is in a certain situation. Martirossian [Mar01, 33ff.] distinguishes between following structural features that can lead to groupthink:

- *The group is insulated.* The group gets the feeling that other members of the organisation are not interested in the decision making process and are thus viewed as outsiders. As a result the group tends to „feel a sense of entitlement and omnipotence".
- *The group lacks an impartial leadership.* Leaders with an emotional decision making style or who are emotionally tied to the organisation[114] will make it hard for the group to make decisions rationally and impartially.

[111] Schein [Sch92] covers the topic of leadership in organisations in depth.
[112] This is based on the assumption that only task-oriented leadership can lead to the productivity required.
[113] In: Mustajoki [Mus99].
[114] This could occur if he/she is a long-time member.

- *The group lacks procedures.* If procedures are missing or circumvented, rational and consistent decision making becomes difficult to ensure. For instance unilateral actions by one or a few group members become accepted by the group and are not reflected upon.
- *The group is homogeneous.* Groups tend toward homogeneity, as people are naturally attracted to others who think like they do. This process is usually slow and is seldomly noticed. Homogeneity leads to groupthink, as conflicting views are missing and decisions are rarely challenged.

Moreover, groups in situations of high stress from external threats tend to show symptoms of groupthink. Similarly groups with a low self esteem, induced by recent failures, excessive difficulties or moral dilemmas are also highly vulnerable.

Major symptoms of groupthink can be observed when the group overestimates its power and morality, when it becomes closed-minded in a sense as it ignores warnings, when it has stereotypical views of the "enemy" and when it is pressured to be uniform. Martirossian names the following uniformity symptoms as to be linked to groupthink:

- A self-censorship of deviations from the apparent group consensus comes with the impression that individual doubts and counterarguments are not important.
- A shared illusion of unanimity concerning judgments conforming to the majority view marginalises other opinions as "destructive and demoralising"[115].
- The group places strong pressure on "disloyal" members, even if their opinion is justified.
- The emergence of self-appointed mind guards that keep "bad ideas" outside of the group.

The groupthink phenomenon can play an important role in information security. Looking at the four structural features and critical situations defined above, one can easily state that InfoSec decisions often happen in similar circumstances, thus leading to groupthink if a group is in charge.

4.3 Summary

In this section, the multiple dimensions of information security are discussed: from the disciplinary point of view, the business, social and technical dimensions can be identified. From the psychological viewpoint, expectations about the role of information systems and their security affect the decision making process of individuals and groups. It is concluded that a group of heterogeneous people can help to incorporate diverse viewpoints into the

[115] Martirossian [Mar01, 40].

decision making process. As one can easily imagine, this plurality can be the source of problems. Therefore the main parameters that can reduce the quality and the efficiency of group decisions are analysed. Most relevant for information security decisions are group polarisation and the „group think“ phenomenons which can alter the quality of the decisions taken in the group.

These basic group decision making flaws should be kept in mind when designing an InfoSec workshop.

5 An assessment of multiple criteria group decision support methods in information security

In chapter 2.1, the multi-disciplinarity of information security was outlined. A way of dealing with this aspect is to allow decision makers to include multiple criteria in their analysis. This chapter discusses the relevance of the use of multiple criteria and of group decision support for the information security process.

Definition of uncertain multiple criteria decisions Keeney and Raiffa [KR76] categorise decision situations using two criteria. The first criteria is defined according to the certainty or uncertainty of the attributes' problems. The second criteria is linked to the dimensions of the problem, whether just one single attribute is enough to describe an alternative, or if two or more attributes are required. Table 3 illustrates this categorisation.

	Single attribute	Multiple attribute
Certainty	x	$\mathbf{x}$
Uncertainty	$\tilde{x}$	$\tilde{\mathbf{x}}$

Table 3: Double dichotomy of decision problems (Keeney and Raiffa [KR76, 27])

Definition of decision support systems Decision support systems (DSS) are tools to support and facilitate decision analysis[116]. Even when DSS are used, decision making is primarily done by humans. DSS should be designed to flexibly adapt to the changing needs of the decision makers[117].

The University of Cambridge manufacturing group categorises 71 decision support systems into the following 4 categories[118]:

1. Information management - gathering, storage, retrieval, and organisation of data, information and knowledge, such as databases, spreadsheets, graphics (histograms and pie charts).

2. Representation aids - tools and techniques that aid visualisation of the data or problem area such as maps, GIS, mind mapping, the Analytical Hierarchy Process (AHP).

3. Choice tools - techniques or tools that analyse or help to narrow the number of choices. These are often referred to as multi-objective decision making (MODM) tools and include goal programming, fuzzy sets, dominance methods.

[116] Mustajoki [Mus99, 25].

[117] Alter 1980, in: Mustajoki [Mus99, 25].

[118] Adapted from http://www-mmd.eng.cam.ac.uk/people/ahr/dstools/classification.htm, in: Tompkins [Tom03, 4].

4. Outcome models - such as value and utility based approaches, cost-benefit analysis, risk analysis, cost-effectiveness analysis, multi-attribute decision making (MADM). These can be predictive or descriptive models that describe impacts under different decisions comprising:

   (a) Descriptive models that can be used to better understand the situation;

   (b) Predictive models that answer "What if?" questions.

This work focuses on the category "outcome models", including cost-benefit analysis and multi-attribute decision making (MADM).

Definitions of group support systems and group decision support systems

A group support system (GSS) consists of a set of techniques, software, and technology designed for the communication, deliberation and decision making in group scenarios[119]. The following criteria characterise GSS: "computer for each participant, software for each task, public screen to focus attention, techniques to manage group activities, network to share information, access to external data, access at any time, at any place and on any platform"[120]. GSS can be classified along time and place criteria, as shown in Table 4:

Place/Time	Same	Different
Same	electronic meeting rooms	shared files, workshift
Different	video conf., chat applications	e-mail, bulletin boards

Table 4: Dimensions of group support systems (Johansen, 1991 in Mustajoki [Mus99, 23])

Group decision support systems are a form of GSS tools: they bring decision makers together and support the decision making in this process. Mustajoki [Mus99, 27-28] names two categories for GDSS: first, systems without decision analytic tools like video conferences and second, GDSS with incorporated decision analytic tools like electronic voting systems. Moreover, GDSS are characterised by asynchronous and synchronous decision making, depending upon whether the information is instantly transmitted and viewed by other decision makers.

In this section will be presented various methods that can be used to support single and group decision making. The presented methods are categorized into those that aggregate criteria values[121] in 5.1 and those that leave it open for the decision maker whether or not

[119] Nunamaker, [Nun97], in: Mustajoki [Mus99, 22].
[120] Nunamaker, [Nun97], in: Mustajoki [Mus99, 22].
[121] For instance, cost and benefit in the case of return on investment (ROI) calculations.

and to what extent criteria are aggregated in 5.2. After their presentation, criteria are defined for their evaluation in the last step.

5.1 Methods for quantitative decision making requiring aggregation

This section presents a few commonly used quantitative methods using a form of aggregation between cost and benefit values for the evaluation for investments in information security.

5.1.1 Cost benefit analysis

According to Clarke [Cla95], cost/benefit analysis (CBA) is a quantitative technique for the evaluation of the effects of members of the economy as a whole, „distinguished from financial evaluation, which is conducted from the viewpoint of an individual firm or agency“. It involves „the identification of all of the costs and benefits arising in relation to a program“, and their measurement. An essential aspect of CBA is that decision makers often need to deal with some costs and benefits that cannot be assigned dollar values. They need to be presented separately, „with as much descriptive information as possible“.

Clarke [Cla95, 10] highlights the special role of opportunity costs, defined as „the benefits foregone from not having done something else with the resources“. Each diversion need to be assigned costs reflecting the best alternative's foregone benefits.

5.1.2 Cost effectiveness analysis

Cost Effectiveness Analysis (CEA) is a standard method for the evaluation of two alternatives which compete for limited resources[122]. It was developed by the military and introduced to clinicians by Weinstein and Stanson in 1977. The following formula produces a result reflecting „the "price" of the additional outcome purchased by switching from current practice to the new strategy“. One can thus calculate the costs in US dollars per life year saved.

$$CE\,ratio \quad = \quad \frac{cost_{new\,strategy} - cost_{current\,practise}}{effect_{new\,strategy} - effect_{current\,practise}}$$

[122] American College of Physicians [Ame00].

The use of CEA is limited to certain situations. For instance, one alternative can be compared to another only if both its costs and effects are lower, or if both are higher. A alternative being cost-effective does not allow conclusions about its ability to „save money“ - being cost-effective and saving money are not casually linked when using CEA.

5.1.3 ROI/ROSI

Purser [Pur04] defines the Total Return on Investment (TROI) metric incorporating risk as follows:

$$\text{Total Return on Investment} = \frac{\begin{array}{l}\text{Generated revenue} \\ -\text{Generated cost savings} \\ -\text{Value of change at risk}\end{array}}{\text{Investment}}$$

Each of the variables are expressed using the same monetary unit. Including risk in the calculation enables to compare alternatives more accurately. However, this calculation is often difficult as appropriate data is often missing.

Iheagwara [Ihe04] defines the Traditional Return on Security Investment (ROSI) as the Annual Recovery Cost (R) reduced by the ALE after the application of the analysed safeguard:

$$ROSI = R - ALE$$

The ALE is defined as follows:

$$ALE = (R - E) + T$$

R	Annual recovery costs from intrusions without safeguard
E	Annual dollar savings gained by using safeguard
T	Annual costs for technology and management

This metric focuses on the monetary valuation of the safeguard and is thus limited to a single dimension.

5.2 Multiple criteria preference rating methods

This section presents commonly used weighting methods for multiple criteria decision making, focusing on the most prominent methods AHP and SMART. An overview of other similar methods is provided.

Analytic Hierarchy Process:

The Analytic Hierarchy Process (AHP) was developed by Thomas Saaty[123]. It is divided into 3 phases:

- First, data for the problem's criteria values and of alternatives is gathered.
- Second, each of the criteria are compared to each other pair by pair. Afterwards, the alternatives are compared pairwise using the defined criteria.
- Third, the collected data is processed resulting in a ranking of the alternatives based on a weighting of the individual criteria.

Additionally, an analysis of the logic and quality of the solution is provided by the AHP method.

Simple multi-attribute rating technique (SMART):

The simple multi-attribute rating technique is similar to the layout of AHP but replaces the pairwise comparisons with a single rating of the alternatives on a scale from 0 to 100[124]. This method is similar to Multiple Rank Ordering (MRO).

Other multiple-criteria rating methods:

Name of the method	Source
SMARTER	Edwards and Barron [EB94]
Multiple rank ordering (MRO)	Akhavi et al. [AH03]
ELECTRE	Roy [Roy91]
SWING	Katrin et al [BEvW91], Butler [But02]
Worth trade-off method	Debeljak [Deb90]
Probabilistic multi-dimensional scaling	Kamenetzky [Kam82]
equal weight average model	Dyer [Dye90]

[123] Saaty [Saa94].
[124] Yap et al. [YRL92].

5.3 Evaluation of the defined decision making methods

This section evaluates the methods presented in 5.1 and 5.2 using the requirements defined in this section.

5.3.1 Evaluation of the single criteria quantitative decision making methods

CBA, cost effectiveness analysis and ROI/ROSI methods have classical drawbacks including their „misleading precision and the scope for analyses to be manipulated to serve vested interests[125]. Often, decision problems include qualitative parameters that are difficult to quantify with precision. They need to be „clearly described“ rather than being quantified by estimations. Moreover, calculations, estimations and assumptions need to be clearly documented.

Clarke [Cla95, 10] even argues that CBA must be itself subject of cost-benefit analysis[126]: thus, constraints on the resources and the time invested in improving the accuracy of the analysis can be found. However, this should not lead to an omission of the CBA, but should lead to improvements like more cost-efficient cost-benefit models.

However CBA is very popular and highly accepted, due to the understandability of the concept by the management[127].

5.3.2 Evaluation of the AHP, SMART and MRO ranking methods

The following criteria for the evaluation of the AHP, SMART and MRO ranking methods can be defined:

Ability to elicit goals and preferences: The rank weighting method helps the decision makers to formulate the goals and preferences in the context of the given problem.

Problem clarification: By structuring the problem, questions and quantification methodologies, methods should contribute to the understanding of the problem area.

Improvement of decision skills: The structure of the method should provide a systematic way to progress with the decision making process. This should yield an improvement in decision skills of the decision makers.

[125] Clarke [Cla95, 10].

[126] This claim is partly relevant for the ROI/ROSI and cost effectiveness approaches, as their costs might be significantly lower than those of a cost benefit analysis.

[127] Mercuri [Mer03, 16].

Comprehensibility of tasks: Every step of the method should be easy to understand and to execute.

Contentment with decision process: Decision makers need to be convinced of the validity and efficiency of the method in use.

Contentment with results: The quality of the results should be convincing to decision makers: in the end they should accept the outcome of the process.

Time requirements: The time needed to accomplish the decision process can be a hindrance if problems have many alternatives and criteria.

Table 5 summarizes results from research work by Yap [YRL92] and Akhavi et al. [AH03].

	Yap [YRL92]		Akhavi et al. [AH03]	
	AHP	SMART	AHP	MRO
Ability to elicit goals and preferences	-	+		
Problem clarification	-	+		
Improvement of decision skills or "Level of agreement"	+	-	+	–
Comprehensability of tasks	-	+		
Contentment with decision process	not significant		-	+
Contentment with results	not significant			
Time requirements	-	+	-	+

Table 5: Comparison between AHP and MRO/SMART (Yap [YRL92] and Akhavi et al. [AH03])

These results show the profiles of the analysed methods: Whereas AHP succeeds in creating a decision making process that leaves the participants agreeing upon the results, it requires a lot of time and - contrary to common belief - contributes less to the understanding of the problem. In addition, it does not yield results that are more satisfying to the decision makers.

5.4 Summary

In this chapter the main methods used for decision support in the context of information security management were presented and evaluated using a set of requirements. On the one side, diverse methods aggregating costs and benefits to a ratio value were discussed. Their main advantages and drawbacks included their high understandability and acceptance, their risk of a misleading impression of precision and their susceptibility to erroneous estimations.

On the other side, methods for the ranking of alternatives using multiple criteria were discussed. It showed that the simpler MRO or SMART methods performed better in terms of decision maker satisfaction, time requirements, problem clarification and the ability to eliciting goals and preferences. However, AHP significantly improves the decision making process and therefore the „level of agreement“ on the results of the decision making process.

Based on this analysis, the decision making model ReMOSST attempts to remain simple and time-efficient while enhancing the decision making process by appropriate means, inculding the limitation of the analysis focus.

6 Requirements for a holistic multiple criteria group decision support workshop

This section presents the main requirements for a quantitative multi-criteria group decision system (GDSS) supported information security risk analysis and portfolio safeguard selection.

It first defines how a quantitative information security risk analysis model should be designed in 6.1. Next, in 6.2, it presents the requirements for a GDSS supporting an information security risk analysis. Finally, 6.3 defines how the selection of portfolios should take place.

6.1 Quantitative information security risk analysis model requirements

This section will present general requirements of a InfoSec risk analysis model inspired by Baer and Zaengerle [BZ00, 69] and Bennett [BK92, 67].

Management orientation: The approach chosen should distance itself from the traditional technical bias[128] and gain management support. This can be achieved by setting goals that are linked to the overall strategic goals of the organisation, by taking existing performance measurement systems into account and by supporting comparisons between targets and actual results.

Completeness: Each part of the company's information system should be considered. This includes not only technical aspects, but also social and organisational issues[129]. The latter are to be seen from the perspectives of users and from the service providers. An approach targeting the company's business processes has to be chosen, as described in sub chapter 3.1.2.

Scalability: The model should be applicable for large as well for small organisations. It adapts to specific organisational and technical specificites.

Comprehensibility: The process' results are to be presented in a easily understandable way. While their link to the defined objectives are clearly identifiable for management, they should be presented to technicians a way that makes their implementation feasible.

Time and cost efficient: As group decisions requires a high amount of resources, group decision process need to consider the costs of each step and for this reason, focus on

[128] See 3.1.3.
[129] See 4.1.

minimizing the total effort.

6.2 Requirements for a quantitative multi-criteria risk analysis group decision support tool

This section presents the main requirements for a multi-criteria GDSS for information security risk analysis.

Mitigation of group decision drawbacks: Group decision making can yield richer and more acceptable decisions while having certain pitfalls[130]. The design of the GDSS should consider these aspects and try to find solutions that mitigate those risks.

Fast convergence of decisions with heterogeneous groups: As described in sub chapter 4, heterogeneous groups tend to turn outwards and find more creative solutions. Decisions may be thus more difficult to reach. The GDSS should be designed to ease aggreement on more contentious issues.

Comprehensibility and user friendliness: The GDSS workflow must be easy to understand. Users ought to be assisted by an intelligent, easily usable GUI. The metrics used should be intuitive and appropriately chosen.

Short preparation time for the technical infrastructure: The technical infrastructure must be easily designed and quick to set up.

Effective and efficient workshop work-flow: The collected data must be easy to aggregate and to compute. Intermediate decisions which reduce the set of alternatives should be suggested and assisted by quantitative user ratings.

Multi-criteria ratings: Providing users the possibility for multi-criteria ratings helps to ensure the multi-disciplinarity of the decision making process and its results. The GDSS should therefore provide this feature. These ratings should be aggregated by the arithmetic mean formula[131]:

$$\overline{x} = \frac{1}{n}\sum_{i=0}^{n} x_i = \frac{1}{n}(x_0 + x_1 + ... + x_n)$$

6.3 Portfolio management and safeguard selection tool requirements

This sub chapter defines the requirements for a tool analysing the data collected by the information security risk analysis GDSS.

[130] See 4.1 and 4.2.
[131] See 3.3.

Pareto optimisation: The portfolio selection algorithm should make use of Pareto optimisation as described in sub chapter 3.3.

Criteria value range definition: In order to limit the scope of the analysis, ranges of criteria values can be set, thus reducing the number of Pareto-optimal portfolios.

Sensitivity analysis: A sensitivity analysis provides an estimate of the robustness of the selected portfolio(s) by varying the relevant input parameters.

7 Development of an information security group decision workshop concept

For the purpose of this work, a solution including an InfoSec risk analysis process and a group decision support tool was developed. The approach is named after the Multiple Objective Safeguard Selection Tool (MOSST) by Thomas Terenyi. „ReMOSST“ is the name of the tool presented in this work, which is inspired by MOSST. The proposed solution has three elements:

- The *holistic ReMOSST workshop*, during which a group of stakeholders with different backgrounds executes a risk analysis covering all relevant perspectives of information security management.
- The *ReMOSST GDSS workshop module*, the decision support system providing a framework for risk analysis to groups of decision makers: chapter 8.2.
- The *ReMOSST GDSS portfolio selection module*, providing advanced post-processing and post-analysis functionality: chapter 8.3.

7.1 Goals of the workshop

The essential goal of the workshop is the cooperative brainstorming and rating of information security risks and safeguards. This constitutes the base for the selection portfolio of information security safeguards after the workshop, described in 8.3. Moreover, the ReMOSST GDSS documents each phase of the workshop, enabling one to retrace every step of the decision making process, long after the actual workshop has concluded. Because of the presence of all relevant stakeholders, the workshop results' completeness and the resulting ex-post justifiability during the implementation can be assured.

In addition to these essential goals, other important objectives can be reached; i.e. quantitatively and qualitatively superior results[132]. In order to comply to the pluri-disciplinarity of InfoSec management, as it has been described in chapter 2, a heterogeneous group is required. Additionally, the completion of the workshop builds a common understanding of information security issues: it induces an organisational learning process and fosters the development of a corporate security culture.

[132] In order to measure this superiority, following criteria can be used: the completeness of the identified risks, of safeguards and of ratings.

7.2 Preparation of the workshop

The preparation of the workshop consists of the definition of the problem area, the collection of data required by the ReMOSST DSS and its interpretation using the problem definition. It therefore builds the base for a selection of important decisions to be covered by the workshop, complying with its definition: "a brief intensive course for a small group; emphasizes problem solving"[133].

The preparation can be divided into 4 phases:

- **Definition of the risk analysis context and goals**
- **Selection of workshop participants**
- **Ex-ante collection of data**
- **Preparation of the workshop's content**

These steps will be described in detail in the following paragraphs.

Definition of the risk analysis context and of strategic information security goals

This first step aims to define the scope of the workshop contents and its goals. It is required for setting the direction of the workshop and for the definition of criteria which will be used to measure its success.

First, the *problem field* has to be delimited by answering following questions:

Who? Organisational responsibility; e.g. a board member, the head of the IT department, etc.

What? Business processes and relevant IT systems; e.g. only the server room and maintenance processes, the company's management information system (MIS), web-based customer services, etc.

Where? the system's geography; e.g. the headquarters offices, the branch offices, etc.

How? Tools and budget restrictions; i.e. safeguards, budget, personel resources available, time frame, etc.

Based on the organisation's strategic goals[134], *strategic IS goals and non-goals* should be defined to give an strategic orientation to the ISM process. They should encompass business, social and technical goals as described in chapter 3.1.3. By taking existing strategic goals

[133] University of Princeton, in [PD05, p.2].
[134] See 3.1.3.

and performance measurement systems[135] into account, the benefit of the workshop for the company can be easier communicated and the workshop can be made more coherent.

Selection of workshop participants

In order to raise the efficiency of the workshop session in terms of quality and quantity of the workshop output, the moderator must select participants according to their knowledge, their "match"[136] and their "key user"-role.

As described in chapter 3.1.3, ISM must take different viewpoints into account. Additionally, it has to be supported by the management and must be accorded enough resources. Therefore workshop participants should be selected to cover the whole spectrum of ISM problems and include a manager in charge of the decisions taken.

Finally one should be aware that the mix of viewpoints on the role of InfoSec among the participants has an effect on results of the workshop[137].

The heterogeneous group should be composed 6 members, with representatives from each of the following groups:

- IT management, e.g. head of IT department
- Top management, e.g. member of the board, chief security officer (CSO)
- Customer relationship management (CRM) and human ressources (HR), e.g. key user
- Operational experts, e.g. InfoSec expert, chief security officer (CSO)

Ex-ante data collection

By collecting relevant data before the actual workshop begins, the focus of the workshop can be laid on a few topics narrowed down in phase 4 of the preparation. Various means are available to gather this information:

- Personal face-to-face discussions with experts, e.g. from management, the IT department, or key-users from HR and CRM
- Analysis of structured checklists and best practices, e.g. the German „BSI Grundschutzhandbuch“ [Bun05]
- Analysis of log files, e.g. intrusion detection systems, mail server, firewall, etc.

[135] Balanced scorecards have a very similar approach that can be very valuable for the definition of strategic ISM goals.

[136] See chapter 4.1.

[137] See chapter 4.1 for a description of the core design ideals influencing the decision making process and the implementation of IS measures.

- Questionnaire

A questionnaire plays an important role as mental preparation for the participants in providing information about contents that will be discussed. The questionnaire is divided into following sections:

- **Individual InfoSec knowledge:** the information of the InfoSec knowledge level of the participants helps the moderator in his/her preparation of the workshop. It also enables a more clear evaluation of the learning performance of the group.
- **Perception of the role of InfoSec in the organisation:** this section provides insight into the role of InfoSec in the organisation, as seen by the workshop participants. Moreover their values regarding information systems, i.e. their core design ideal as defined in 4.1, can be analysed.
- **Critical success factors for information security management:** this provides insight into the criteria that are identified as factors relevant for the success of InfoSec.
- **Naming of assets, threats and safeguards:** The gathering of risk analysis items helps the moderator during the preparation of the workshop.

The questionnaire used during the field study can be found in A.

Preparation of the workshop's content

The data collected during the last three steps can be entered in the ReMOSST DSS: it is an important moment of the risk analysis as the interpretations of the collected data shapes the rest of the process and its outcome. The data to be entered covers all areas of the brainstorming module (i.e. cost and value categories, goals, assets, vulnerabilities, threats, risks, safeguards and dependencies): this helps reducing the time requirements of the workshop and to focus on the key tasks and items that requires a group.

7.3 Realisation of the workshop

Time line of the workshop:

The workshop can be divided into following phases[138]:

- 15 min: preparation of the workshop[139]

[138]The description of consistency requirements, input/output data of the following phases is described in detail in 8.2.

[139]The preparation time depends on the available technical infrastructure: for this best-case estimate, a functioning ethernet network, a projector, a server and a client per participant are assumed.

- 10 min: introduction[140]
- max. 2h25 min: risk analysis workshop[141]
  - 10 min: value and cost categories
  - 20 min: information security management goals
  - 45 min: assets, vulnerabilities and threats
  - 10 min: coffee break
  - 20 min: risks
  - 30 min: safeguards
  - 10 min: safeguard dependencies
- 10 min: Wrap-up and feedback[142]

The ReMOSST workshop can be executed in a comparably short period of time: two to three hours. Nevertheless, because of this dense structure and the strong links between the phases, all participants have to stay present for as long as possible. If some participants must leave, they should avoid interrupting the first hour of the risk analysis.

The ReMOSST workshop requires an array of technical equipment, as shown by figure 18:

- Server PC: A PC or laptop connected to the Ethernet LAN network and to the video projector is running the Odin MODSS server application with the ReMOSST server brainstorming module.
- Video projector: By showing the user interface (UI) of the Odin MODSS server application to all participants, steps executed by the moderator on the server PC can be made visible to the group[143].
- Ethernet LAN network: The LAN is necessary to connect the clients to the server in order to exchange data over .NET Remoting.
- Client PCs: The client PCs or laptops need to be connected to the LAN network and configured to be able to communicate with the server using .NET Remoting.

[140]The introduction starts when all participants are present. A standardised presentation is run by the moderator.

[141]The factors influencing the time estimate are described in more detail in 8.2.

[142]The wrap-up phase and feedback phase are important steps for reflection on the results and the outcome of the workshop.

[143]For instance, rating results are discussed in the group and items are selected in front of all group members. If consensus has not been reached, the group or the moderator can decide to repeat the rating step.

The first step of the workshop consists in setting up this infrastructure and testing it. Next, the participants can be shortly are met and welcomed. Following is the risk analysis making use of the ReMOSST DSS. In every step, it alternates group brainstorming (on a flip chart or directly on line using ReMOSST DSS), individual rating of alternatives and the selection of alternatives in front of the group via presentation video projector.

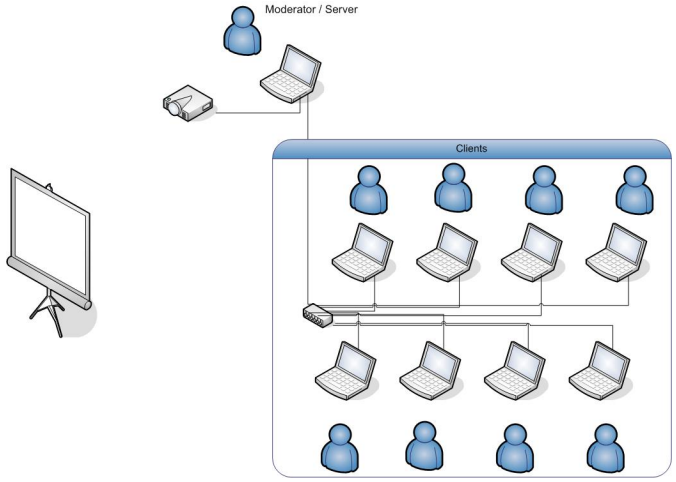


Figure 18: The technical infrastructure required by the ReMOSST Workshop

Workshop phases and steps:

Figure 19 is an outline of the main phases and steps of the ReMOSST workshop described below.

Each step of the work flow defines, rates and selects an important element of the risk analysis. For the sake of clarity, the ReMOSST-GDSS phases[144] are described only summarily briefly in this section.

Value and cost categories: In this step asset value and safeguard cost categories are defined.

Strategic goals: This step enables the definition of the scope and the focus of the workshop risk analysis in a cooperative way. These goals should reflect the main business requirements for the continuity and information security of the main business functions relevant for information security. After the definition step, goals can be rated individually on a qualitative scale and selected. Chapter 3.1.3 presents a few generic goals created in this phase.

[144] See 8.2.

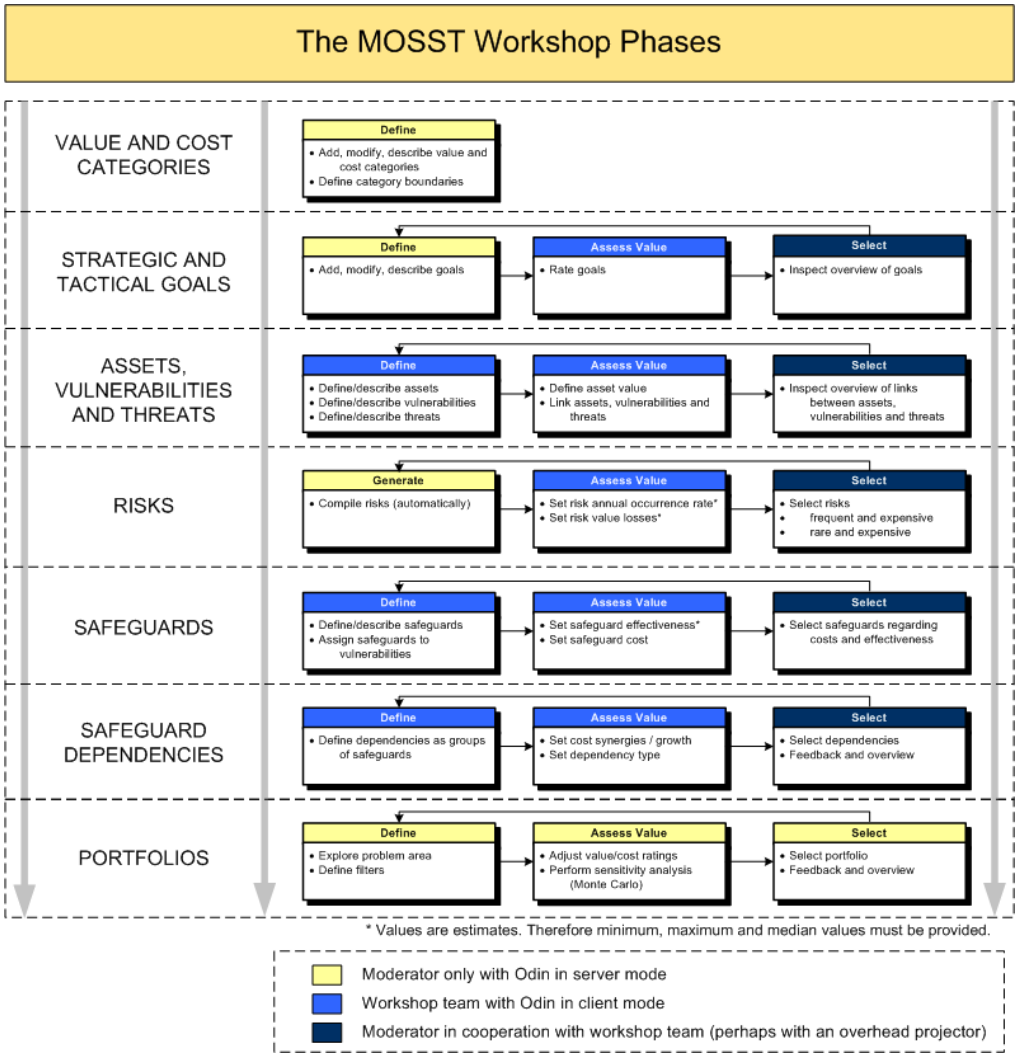


Figure 19: Detailed workshop layout

Assets, vulnerabilities and threats: The definition of these three object types builds the base of the risks' definition in the following step. Asset must be valued: these values help in estimating the potential impact of an incident, modelled in the next step.

Risks: As defined in chapter 2.2.5, the cross-product of assets, threats and vulnerabilities build the domain in which risks can be modeled. As a first step, risks can be defined by associating vulnerabilities to threats and assets. Then, the estimated annual occurrence rate (ARO) and impact of an incident can be entered. Finally, the moderator can visualize the aggregated risk ratings and selects the most frequent and dangerous[145] risks.

[145]This is expressed in terms of asset value exposure.

Safeguards: Based on the last step's risks, safety measures can be identified in order to avoid, lower or divert risks. Therefore, safeguards are rated by their efficiency measured in relative factors defining their risk likelihood and impact reduction. Safety measures depicted in figure 14 on page 33 are modeled using following approach:

- Deterrent controls, reducing likelihood:

  By reducing the frequency of occurrence of a risk by the factor R the expected ALE of the given risk is reduced by ALE = initial frequency x Impact x R = initial ALE x R

- Preventative controls, reducing the impact:

  Similarly to the deterrent controls a reduction of the impact by R reduces the ALE by the same calculation.

- Detective controls, enabling preventative controls:

  Detective controls are assumed to be without effect on the ALE, but can be combined with preventative controls which they trigger using dependencies in the next step.

Each safeguard has costs, which are based on the cost categories of the first step. Marking safeguards with a mandatory flag ensures that they are selected in all portfolios. This helps in dealing with special situations, for example when:

- External factors influence future risks by acting like safeguards. For instance, when the neighbour parking lot is hiring a guard.
- Another example would be if the management has already decided to implement an organisational change, which will alter risks.

Safeguard dependencies: Safeguard dependencies enable the linkage of safeguards. This helps in modeling diverse relationship between information security investments:

- "min"-dependency: At least a given number of safeguards has to be selected out of a given group.
- "max"-dependency: At most a given number of measures can be selected out of a given group.

Moreover each of the defined dependencies can be valued in terms of the synergies they effect in terms of safeguard costs.

Pareto-optimal portfolios: By being showed a first draft of some modeled portfolios[146], the participants can get a first impression of the possible outcomes of the portfolio analysis which will be completed after the workshop.

7.4 Wrap-up phase

The wrap-up phase comprises the portfolio analysis, described in depth in chapter 8.3, a questionnaire to assess the opinion of the participants concerning the workshop and the writing of a report about the results of the workshop.

Wrap-up questionnaire The wrap-up questionnaire aims to evaluate if the workshop's requirements defined in 6.1 and 6.2 have been met. It is structured accordingly in the following sections:

- **User-Friendliness:** The tool's GUI usability is evaluated: interactions that appeared too cumbersome can be identified and improved.
- **Comprehensibility:** This helps in identifying the aspects of the workshop and the ReMOSST DSS that may have been difficult to understand for workshop participants.
- **Completeness of the risk analysis:** This asserts if the participating specialists judge that the risk analysis covered all relevant aspects and was therefore complete.
- **Contentment with the results:** This section tries to determine how the workshop was accepted by the participants and if it should be repeated or improved.

Section B presents a questionnaire used during the field study.

Workshop report The workshop report presents the results of the risk analysis and a concrete strategy and implementation/testing plan. The workshop report written in the context of the case study can be found in 9. It is structured in three main phases:

Impact assessment: This step presents the main findings of the risk analysis and defines priorities for the recovery after incidents. Its analysis begins with the main business functions and the requirements for their continuity and information security.

[146] See chapter 8.3 for details of portfolio computation.

Strategy development: The development of an adequate strategy including management support, a team taking the responsibility for implementation and a complete plan is often necessary in order to successfully put the information security safeguards in place.

Implementation and testing plan development: Finally, a plan for the implementation of the information security safeguards must be developed. This plan includes project resources, advance arrangements, and a description of the information security safeguards. The latter also includes information about the time of the implementation, who is responsible, etc.

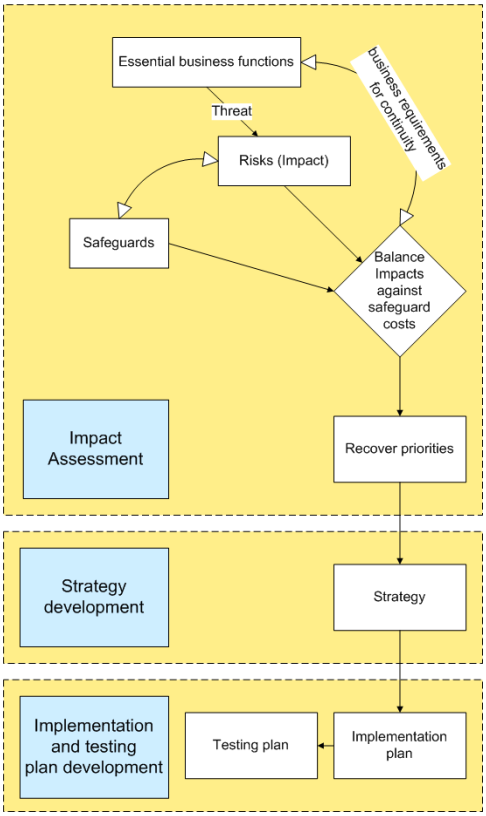


Figure 20: Steps of the analysis and structure of the business continuity report

Follow-up and implementation: After the completion of the report, it is presented to the board or a representative and the recommended set of safeguards is presented. Each safeguard is decided upon individually, which could therefore lead to a situation in which a portfolio that has been identified as optimal is not implemented fully. The report should therefore present a handful of safeguards and communicate which combinations make the most sense - based on the results of the portfolio analysis.

8 Implementation of a GDSS for efficient information security workshops

In the course of the research work for this thesis, the group decision support system (GDSS) ReMOSST was implemented. Its aim is to support information risk analysis workshops and safeguard selection trough quantitative multi-criteria ratings and portfolio management methods.

The ReMOSST GDSS uses the Odin GDSS Framework, which provides basic services like user management, decision situation management and client/server graphical user interfaces (GUI).

This chapter presents in a first step the implementation layout including Odin GDSS, the ReMOSST plugin, and the client/server logic in 8.1. In section 8.2, it describes the ReMOSST group brainstorming module, followed by the InfoSec portfolio selection module, presented in 8.3.

8.1 Overview of the ReMOSST GDSS

The ReMOSST GDSS is a tool built upon the Odin Decision Support framework developed by Thomas Mikscha at the Institute for Information Systems at the Technical University of Vienna[147].

Figure 21: The Odin splash screen

Its architectural structure is described in figure 22.

Odin framework: The Odin Multiple Objective Decision Support System (MODSS) is a framework developed by Thomas Mikscha [NM05] in 2005. It is developed in .NET C# and uses Microsoft SQL Server 2000 for persisting its data. It provides diverse basic services such as user and session management, a plugin framework and standardised controls.

[147] Neubauer and Mikscha [NM05].

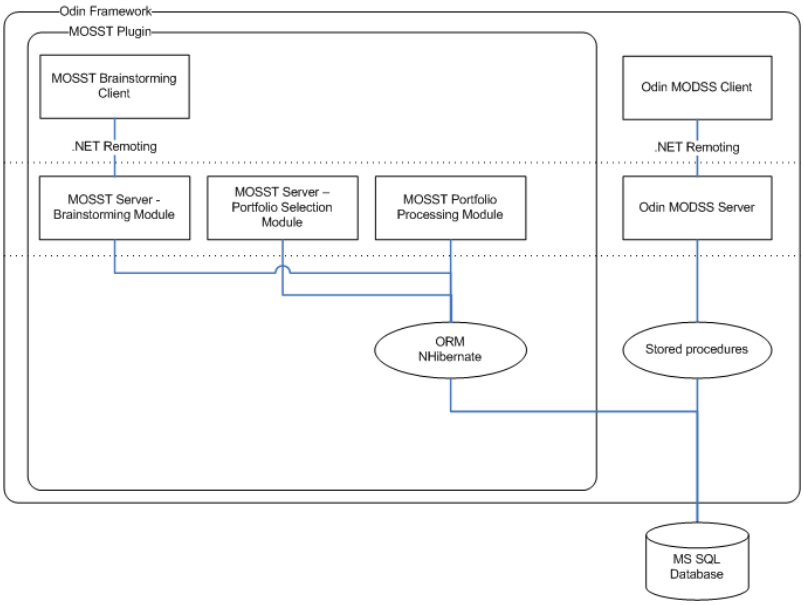


Figure 22: The Odin and ReMOSST architecture

Odin MODSS server: The Odin MODSS Server handles the connection to the MSSQL database, registers .NET Remoting Objects and implements user registrations. It provides user interface access to the specific administration backends, to portfolio processing and to a selection graphical user interfaces (GUI) for each plugin.

Odin MODSS .NET Remoting clients: The Odin MODSS Client application connects to the Odin MODSS Server by .NET Remoting and prompts access via an authentication dialog. After the login, the user can access password-protected rating sessions, proceed to ratings and send them to the server, which persists the data to the database for further processing.

Microsoft SQL database: The Odin MODSS Server can access Microsoft SQL Server 2000 databases. Odin uses stored procedures which have the advantage of being faster and more secure.

NHibernate object-relational mapper (ORM): The ReMOSST plugin is implemented using the NHibernate object-relational mapper (ORM). Quoting the hibernate.org Website:

> Hibernate is a powerful, high performance object/relational persistence and query service. Hibernate lets you develop persistent classes following object-oriented idiom - including association, inheritance, polymorphism, composition, and collections.

ReMOSST server plugin - brainstorming module: The ReMOSST server brainstorming module, described in section 8.2, controls the flow of the group brainstorming and facilitates the rating session. Each phase of the risk analysis is divided into 3 steps. The first step is group brainstorming: the group shares ideas then describes items qualitatively. Each participant sees the entries of his colleagues in near-realtime. Next, each person rates the entered items independently. These ratings are aggregated in the final step: depending on mean rating and group consensus, the moderator decides which items should be selected and which may require further discussion during another decision making cycle.

ReMOSST client .NET Remoting plugin - brainstorming module: The ReMOSST client plugin brainstorming module is derived from the server brainstorming module and is restricted in function. For instance, it is not possible for a client to delete entries. It has no direct link to the database and communicates with the server via .NET Remoting.

ReMOSST server plugin - portfolio processing module: The portfolio processing module computes the valid and Pareto-optimal portfolios using data from the brainstorming module. After generating all optimal portfolios, they are persisted to the database. Two modes are available: the first compares portfolios using a simple mean value calculation, the second computes estimated variances by Monte Carlo simulation and compares portfolios confidence intervals[148].

ReMOSST server plugin - portfolio selection module: The portfolio selection module uses portfolio data saved by the ReMOSST portfolio processing module. It visualises optimal portfolios and offers further tools for finding one or more adequate portfolios. Additionally a sensitivity analysis can be performed using a Monte Carlo simulation[149].

8.2 The ReMOSST brainstorming module

The ReMOSST brainstorming module enables a group of decision makers to quickly assess the risks and safeguards relevant to the information security of their organisation. Its workflow is structured in three elemental steps: first, during brainstorming, the group enters as many items as they deem appropriated. Second, each participant rates the items individually and secretly. In the third step, the ratings are aggregated and quickly analysed. During a group discussion based on the ratings' analysis, the group decides which items are to be selected. If needed, the brainstorming and rating steps can be repeated.

[148] This is described in more detail in (8.3.1).
[149] See 8.3.3.

This section presents each of the steps modeled by the ReMOSST brainstorming module:

1. Cost and Benefit/Value Criteria
2. Strategic InfoSec Goals
3. Assets, Vulnerabilities and Threats
4. Risks
5. Safeguards
6. Safeguard dependencies

In the following sections, each of these phases is presented using the following schema:

- **Prerequisites:** This defines the data required by ReMOSST before the phase can begin.
- **Phase description**
- **Consistency requirements:** This defines how data needs to be entered in this phase in order to be useful during the next phases.
- **Client-server interaction:** This defines how clients can post items and ratings, how these inputs are processed and how the the aggregation of client ratings does take place.
- **Time requirements**

8.2.1 Cost and benefit/value criteria

Prerequisites: In the Odin Server framework, a Odin decision situation and a linked rating session have to be created and selected in the ReMOSST server brainstorming module. Odin clients must have signed on and loaded the password-protected Odin rating session.

Phase description: The moderator user can define two sets of criteria: First, a set of safeguard costs, which are used to quantify the costs of safeguards and the synergies of dependencies. Next, value criteria can be defined. They will be the base for determine asset values, risk impact values and safeguard effectiveness ratings; finally, portfolio values will be computed by the ReMOSST processing module using these value criteria.

Cost and value categories are defined by a name and a unit: for instance, monetary costs will be measured in euros or dollars. A description can be provided, documenting the definition and the metrics's application context.

Consistency requirements: Cost and value categories have to be defined at the beginning of the workshop in order to guarantee data consistency throughout the whole session.

Client-Server interaction: Clients do have access to this step, nevertheless they cannot edit and save cost and value categories: this can be done by the moderator user and witnessed by the group.

Time requirements: The following table provides guidance on how long this phase takes on average:

Description	Estimate in min.	Calculation
Introduction	2	
Discussion	6	30 sec. x 12 categories
Sum:	8	

8.2.2 Strategic INFO-SEC goals

Prerequisites: This step has the same prerequisites as the previous one.

Phase description: In the first step, clients can enter and describe diverse goals, which are to be met by the risk analysis and a information security management process in general. A tree structure supports the structuring into different layers: ReMOSST defines first-level goals as "strategic" and sub-goals as "tactical".

Next, the goals entered during the brainstorming step are rated individually on a qualitative scale from 1 to 5[150].

Finally, the moderator user can view an aggregated view[151] of all client ratings and select the goals for which a favourable consensus has been reached.

This phase is not required for the portfolio processing and selection steps, as the goals do not contain any quantitative information. It clearly defines the context for the identification of assets, threats, vulnerabilities and safeguards.

[150] On this scale 1 is the worst rating, 5 the best.

[151] The aggregation of goal ratings is implemented by a mean function ignoring invalid ratings, defined by the value „-1“.

Consistency requirements: The structuring of the goals tree is essential if short-term tactical goals are to be viewed in relationship to long-term strategic information security goals.

Client-Server interaction: The goal phase follows the general ReMOSST workshop pattern: first, the client group carries out a goals brainstorming step, and then the goals are rated by each client individually. Finally, goals are selected by the moderator.

Time requirements: The following table provides guidance on how long this phase takes on average:

Description	Estimate in min.	Calculation
Introduction	2	
Discussion	6	30 sec. x 10 goals
Manipulation	5	1 min. x 5 goals
Rating	2	10 sec. x 12 goals
Selection	6	3 min x 2 discussed goals
Sum:	21	

8.2.3 Assets, vulnerabilities and threats

Prerequisites: Before proceeding with the identification of assets, value categories should to be defined in the first step. Moreover, goals should be set as they can be linked with assets, vulnerabilities and threats.

Phase description: In the first step, participants can enter assets, vulnerabilities and threats in a tree structure. They can structure the entered data using folders. Each entered item is defined by its name, its description and - if it is an asset - its multi-criteria value. Moreover, each item can be associated with a goal from the previous step. This link provides very valuable information during and after the workshop and helps to justifying why the item has been taken into account.

In the next step, assets and vulnerabilities are rated in the same fashion as goals: using a qualitative scale from 1 to 5. Threats are rated using the next period's estimations of their annual rate of occurrence (ARO). Because of this value's uncertainty, minimum, median and maximum estimations can be entered. The threats' ratings of the ARO is the default value for related risks' frequency rating.

Lastly, the server plugin can show an aggregated view[152] of all client ratings and then selects the items for which a favourable consensus has been reached.

Consistency requirements: By linking items to goals, the consistency and understandability of the brainstorming data can be improved. Client ratings should to be filled out without gaps.

The rating of threats' estimated annual rate of occurrence is necessary for deciding which threats are to be selected. In addition they constitute default values for risks' annual rate of occurrence, thus improving the efficiency of the risk analysis if available.

Client-Server interaction: This step follows the standard ReMOSST pattern, as described in 8.2.2.

Time requirements: The following table provides guidance on how long this phase takes on average:

Description	Estimate in min.	Calculation
Introduction	2	
Discussion	10	15 sec. x 20 assets+10 vulns+10 threats
Manipulation	10	1 min. x 10 items
Rating	8	10 sec. x 48 items
Selection	16	2 min x 8 discussed items
Sum:	46	

8.2.4 Risks

Prerequisites: As defined in chapter 2.2.5, risks are the cross product of asset values, vulnerabilities and threats. In order to create risks, these item sets have to be completely identified.

Phase description: As risks are defined as the cross product of assets, vulnerabilities and threats, they are identified by creating links between these item types. First, the moderator user selects each vulnerability and links it to assets and threats in order create risks. This risk creation step occurs in front of the group, which helps to build a common view of the possible risks.

[152] The aggregation of ratings is implemented by a mean function ignoring invalid ratings, defined by the value „-1“.

This in turn helps each participant when it comes to rate the risks in the next step: first, the annual rate of occurrence of each risk has to be estimated using minimum, mode and maximum estimations. Next, multi-criteria impact-ratios for each risk define the potential loss in asset values in the case of a successful attack.

Finally, risks are visualized in a two-dimensional risk table shown in Figure 34: on the X axis, risks are sorted by their aggregated ARO rating, on the Y axis by their aggregated impact value rating[153]. Red, yellow and green color zones are defined as follows:

Red: High ARO, high impact. These risks need to be dealt with urgently, as they pose a major threat to the company's information security.

Yellow: Low ARO, high impact. Risks in this category occur rarely, but cause high damage. They should be considered carefully, as items of importance might inadvertently be omitted.

Green: Low impact, high or low ARO. Risks in this category can be reduced using standardised approaches including check-lists and best practices. It should be noted that risks with very high ARO can cause high cumulative damage - even though their impact is limited[154].

An auto-select mode chooses automatically all risks located in the red and yellow cells.

Consistency requirements: Client ratings should be filled out without leaving blanks, in order to ensure homogeneously distributed results. The ratings of risks are fundamental in the rating of safeguards, as well as the processing and selection of portfolios.

Client-Server interaction: This phase differs from the standard pattern as its brainstorming step is done by the server in front of the other participants.

Time requirements: The following table provides guidance on how long this phase takes on average:

[153] The aggregation of ARO and impact values uses a simple sum algorithm, ignoring invalid ratings defined by the value „-1".
[154] See chapter 2.2.

Description	Estimate in min.	Calculation
Introduction	2	
Manipulation	3	3 sec. per link x 8 vulns x 5 links
Rating	15	20 sec. x 50 risks
Selection	2	20 sec. x 6 value categories
Sum:	22	

8.2.5 Safeguards

Prerequisites: The definition and rating of safeguards require cost categories to define safeguard costs and risks to quantify the effectiveness of safeguards.

Phase description: This phase is divided into one brainstorming step, two rating steps and one final selection step. First, safeguards are created by participants and structured in a safeguard tree using categories and subcategories. These safeguards can be assigned multi-criteria costs and linked to vulnerabilities and threats. These links define the scope of risks against which the safeguards offer protection.

The first rating step aims to quantify the ARO-reduction factor of safeguards. It uses the links defined in the first step to filter the relevant threats and risks. The clients can rate the overall reduction factor for all targeted risks. The second rating step deals with the impact reduction factor of safeguards. ReMOSST provides users a aggregated figure of the endangered asset values of the targeted risks for orientation. The final selection step computes aggregated ratings of the ARO and impact reduction ratings[155].

Consistency requirements: Client ratings have to be filled out without leaving blanks, otherwise the aggregation algorithm of the final step will fail. Both ratings are relative ratings as percent points.

Client-Server interaction: This step follows the standard ReMOSST pattern, as described in 8.2.2.

Time requirements: The following table provides guidance on how long this phase takes on average:

[155]The aggregation of safeguard costs, ARO and impact reductions uses a simple sum algorithm, ignoring invalid ratings defined by the value „-1“.

Description	Estimate in min.	Calculation
Introduction	2	
Discussion	8	20 sec. x 24 safeguards
Manipulation	5	30 sec. x 10 safeguards
Rating	10	20 sec. x 30 safeguards
Selection	2	20 sec. x 5 safeguards
Sum:	27	

8.2.6 Safeguard dependencies

Prerequisites: Safeguard dependencies are tied to safeguards: it is therefore necessary that safeguards are completely defined and rated. Moreover, if synergies are defined, cost categories are required to define (dis-)economies of scale.

Phase description: In the first step, dependencies are defined by their name, their type and the quantity of safeguards included in the dependency.

Following dependency types are modeled in ReMOSST:

- „At most n out of m safeguards (max)“
- „At least n out of m safeguards (min)“
- „Synergies“ are linked to one of the previous two dependency types. Choosing a synergy type activates the synergy rating of the current safeguard in the next step.

The dependency rating step is composed of a quantitative rating of synergies associated with dependencies. These synergies are absolute values representing the safeguard costs saved in the respective cost units. Next to each synergy, the cumulated safeguard costs are indicated. Finally, decision making during the selection step is supported by aggregated synergy values and aggregated qualitative client ratings. This phase is not stringently required for the processing and selection of portfolios, it is however very helpful in situations with complex safeguard investment decisions. For instance different backup frequencies could be modeled using an equal number of safeguards, which would then be mutually exclusive and modeled by an „at most 1 out of m safeguards“ dependency.

Consistency requirements: Client ratings have to be filled in without leaving blanks, otherwise the aggregation algorithm in the final step will fail.

Client-Server interaction: This step follows the standard ReMOSST pattern, as described in 8.2.2.

Time requirements: The following table provides guidance on how long this phase takes on average:

Description	Estimate in min.	Calculation
Introduction	2	
Discussion	2	30 sec. x 4 dependencies
Manipulation	2	40 sec. x 3 dependencies
Rating	2	20 sec. x 6 dependencies
Selection	2	20 sec. x 2 dependencies
Sum:	10	

8.3 The ReMOSST portfolio analysis module

After the workshop, the moderator analyses the collected data in order to select portfolios and recommend a further course of action based on results delivered by the ReMOSST portfolio analysis module. ReMOSST divides this into two tasks: „processing“ and „selection“, outlined in figure (23).

First, the initial set of Pareto-optimal portfolios[156] is computed, as described in 8.3.1:

- Step 1: each combination of safeguards which does not comply with the restrictions imposed by the defined dependencies and mandatory conditions is filtered out.
- Step 2: the remaining valid portfolios are compared to each other in order to select the Pareto-optimal portfolios.

Next, the moderator can visualise the Pareto-optimal portfolios and define budget restrictions to define narrower problem bounds and proceed with the analysis. These interactions are discussed in 8.3.2.

After a few iterations, the moderator selects a handful of portfolios for further evaluation. In order to examine the possible effects of uncertainty on the chosen portfolios, the moderator can follow up with a sensitivity analysis of Monte Carlo simulation data, which is discussed in depth in 8.3.3.

[156] as defined in 3.3.

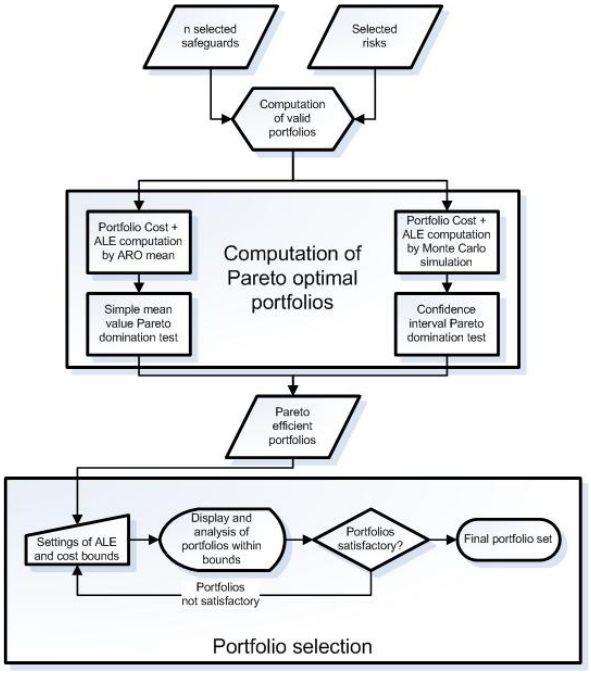


Figure 23: Flow chart of ReMOSST portfolio processing and selection steps

8.3.1 Initial processing of portfolios

The processing step starts with defining all possible portfolios by initializing the safeguard selection vector $I(S_j)$ required by the ALE calculation presented in 5. Given n safeguards, then 2^nportfolios can be defined.

Computation of valid portfolios

The ReMOSST model defines the validity of a portfolio by checking the following conditions:

- Are all safeguards marked as "mandatory" included in the portfolio?
- Does the portfolio meet the restrictions defined by the dependencies?
  - In the case of a "min"-dependency, a minimum amount of safeguards out of a given group has to be selected in each portfolio.
  - In the case of a "max"-dependency, a maximum amount of safeguards out of a given group has to be selected in each portfolio.

Computation of Pareto optimal portfolios

The group of valid portfolios needs to be filtered in order to find the "best" portfolio(s),

with the lowest costs and the lowest ALE. Nevertheless, cost and ALE are both defined by multiple criteria, which cannot be aggregated to a single unique value. Thus, the comparison and rating of portfolios has to make use of the Pareto criterion, declaring that a portfolio is "dominated" only if it is inferior by all cost and value categories. All portfolios which are not dominated are Pareto-optimal[157].

ALE values are computed using the following formula, described in 5:

$$ALE = \sum_{i=1}^{n}(F_0(B_i) \cdot D_0(B_i) \cdot \prod_{j=1)}^{m}(1 - E_f(B_i, S_j) \cdot I(S_j)) \cdot (1 - E_d(B_i, S_j) \cdot I(S_j)))$$

$$I(S_j) \quad Binary\ function\ indicating\ that\ safeguard\ j\ is\ selected$$

This ALE formula and the cost sum are illustrated by the following simplified figure:

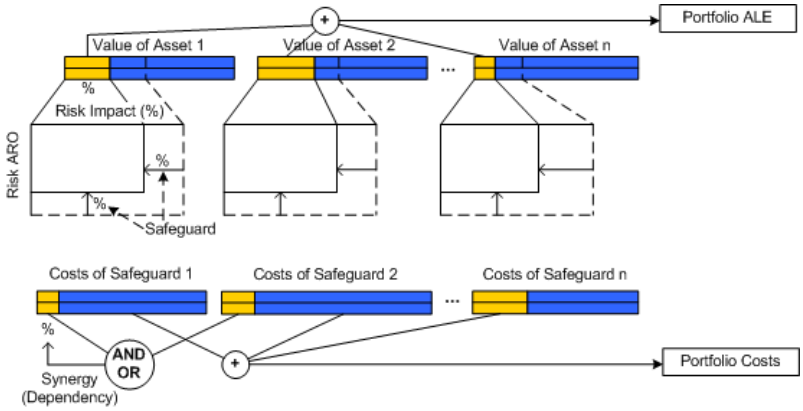


Figure 24: The ReMOSST model portfolio aggregation

The ALE formula is implemented by the following algorithm[158]:

[157] See chapter 3.3 for a complete description of the Pareto-optimality criterion.
[158] In E, the ALE and costs of a sample portfolio are calculated using this algorithm.

Algorithm 1 ReMOSST ALE computation algoritm

```
ALE(Portfolio p, List all_assets) {
 foreach asset in all_assets {
  foreach asset_value in asset.Values {
   foreach risk in asset.Risks {
    foreach safeguard in all_safeguards {
     if safeguard fights against risk, compute ARO and Impact reductions;
    }
     compute ALE value with risk ARO (reduced by safeguards' ARO reductions) and
impact values (reduced by safeguards' impact reductions);
   }
   sum all ALE values do an aggregated portfolio ALE value;
  }
 }
 return set of aggregated portfolio ALE values;
}
```

The portfolio ALE is the sum of all asset values times the impact of a risk times the risk's annual rate of occurrence (ARO). The portfolio costs can be obtained by adding all safeguards' costs and subtracting the value of synergies. Nevertheless, due to the uncertainty of the ratings of risks' ARO and safeguards' relative ARO reduction, results from this analysis can be easily discounted. Therefore two modes are available for the computation of Pareto-optimal portfolios, as depicted in figure 23:

- First, a simple straight forward approach computes the ALE values using the mean ARO of each risk:

  $mean = (a + b + c)/3$, where a, b and c are the three parameters of the triangular distribution. Algorithm 2 describes how Pareto domination is determined

Algorithm 2 Pareto domination with mean risk's ARO approach

```
function Dominates(Portfolio p, Portfolio q) {
  //First find out if there is one cost or ALE criteria that could mean that q is better(low
values).
 for each cost category : if (mean_costs(q) < mean_costs(p)) return FALSE;
 for each ALE category : if (mean_ALE(q) < mean_ALE(p)) return FALSE;

 //If here, this means that p is almost as good (low values) as q.
 //Next find out if there is one cost or ALE criteria that p is better (smaller) than q.
 for each cost category : if (mean_costs(q) > mean_costs(p)) return TRUE;
 for each ALE category : if (mean_ALE(q) > mean_ALE(p)) return TRUE;
}
```

- A second approach computes portfolio's ALE distributions by setting each risks' ARO to a random value computed by Monte Carlo simulation, as described in 8.3.3.

It then compares these distributions. Only if Pareto domination can be observed for each of the simulated values can be assumed for the whole portfolio. Algorithm 3 presents the implementation of this approach.

Algorithm 3 Pareto domination with Monte Carlo simulation approach

```
function Dominates_MC(Portfolio p, Portfolio q, int iterations) {
 //First find out if there is one cost or ALE criteria that could mean that q is better (low values).
 for each cost category : if (mean_costs(q) < mean_costs(p)) return FALSE;

 //Next line means: if the worse ALE value of q (max) is better (smaller)
 //than the best of p (min), then q is not dominated by p.
 for each ALE category : if (max_ALE(q, iterations) < min_ALE(p, iterations)) return FALSE;

 //If the algorithm comes to this point, this means that p is almost as good (low values) as q.
 //Next: find out if there is one cost or ALE criteria showing that p is better (smaller) than q.
 for each cost category : if (mean_costs(q) > mean_costs(p)) return TRUE;

 //Next line means: if the best ALE value of q (min) is worse (bigger)
 //than the worse of p (max), then q is dominated by p.
 for each ALE category : if (min_ALE(q, iterations) > max_ALE(p, iterations)) return TRUE;
}
```

8.3.2 Interactive selection of portfolios

This step reduces the analysis workload by excluding outliers and unrealistic or unacceptable portfolios. Finally a set of portfolios is selected and can be analysed following a Monte Carlo simulation of the ALE values.

Setting of ALE and cost upper and lower bounds: By defining bounds to ALE values, the analysis can be limited to Pareto-optimal portfolios that are acceptable to the decision maker, in terms of his risk tolerance. By limiting the scope of costs, the decision maker can model budgetary restrictions and the scarcity of resources. For instance, if only two specialists are available to implement safeguards, the upper bound of the cost category „working hours“ will be limited to the estimated amount of working hours of these employees during the next period.

Display and analysis of portfolios within bounds: After modifying the cost and ALE value bounds, portfolios fitting within these limits are highlighted by a green background. The selected Portfolios can be analysed using the following tools:

- A list shows the number of portfolios for each safeguard and helps to understand which safeguards can be considered as most important to implement within the setting of the defined bounds.
- A bar graph underneath the bounds list shows the distribution of the costs or ALE values of all portfolios and the selected bounds category. By activating a check-box, values of portfolios that are not within the bounds can be hidden.
- Lists show the safeguards, ALE and COST values of the current portfolio.
- A one dimensional graph shows how portfolio values are distributed.
- A sensitivity analysis using a Monte Carlo simulation, described in 8.3.3, shows the distribution of a given ALE value.

Decision if portfolios are satisfactory: If the following criteria are matched, a set of portfolios or a single portfolio can be selected and be proposed to the management:

- satisfactory ALE reductions
- acceptable costs
- if more than one portfolio is chosen, the selected safeguards and their prevalence in these portfolios should allow clear recommendations.

8.3.3 Monte Carlo simulation and sensitivity analysis for the ReMOSST model

This section presents the implementation of Monte Carlo simulation for the ReMOSST model and how computed data is visualised and analysed.

Monte Carlo simulation in the ReMOSST model

Due to the complex uncertainty issues during the computation of the portfolio's optimality, a Monte Carlo simulation can provide an experimental estimation of the robustness of the computed portfolio VaR Values. According to the NIH [Nat], a Monte Carlo simulation is:

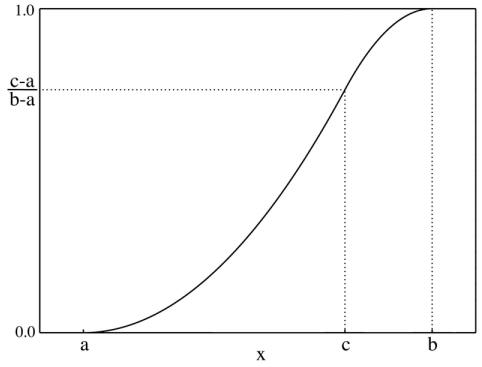
„a technique used in computer simulations that uses sampling from a random number sequence to simulate characteristics or events or outcomes with multiple possible values.“

The goal of the Monte Carlo simulation is to provide an estimate for the integral formula $g(X)$ which values are distributed according to $p(X)$ over the value domain Ω:

$$\begin{aligned} G &= \int_{\Omega} g(X)p(X)dX = \langle G \rangle \,, \\ p(X) &\geq 0 \\ \int_{\Omega} p(X)dX &= 1 \end{aligned}$$

In the context of the ReMOSST model, a Monte Carlo simulation helps to simulate distributions of the portfolio's values by letting the risk's occurrence rate vary between the bounds defined during the rating of the risks in the ReMOSST brainstorming module.

The ReMOSST Portfolio Selection tool computes the ALE formula described in 8.3.1, replacing the uncertain components $F_0(B_i)$ and $E_f(B_i, S_j)$ with the inverse formula of the cumulative distribution function of the triangular distribution:



$$\begin{aligned} CMF(a,b,c) &= \frac{(x-a)^2}{(b-a)(c-a)} \quad for \quad a \leq x \leq c \\ CMF(a,b,c) &= 1 - \frac{(b-x)^2}{(b-a)(b-c)} \quad for \quad c < x \leq b \end{aligned}$$

Figure 25: Cumulative distribution function of the triangular distribution

The inverse cumulative distribution function can be written as $x = \sqrt{CMF(a,b,c)(b-a)(c-a)} + a$ if $0 \leq CMF(a,b,c) \leq \frac{c-a}{b-a}$ and $x = b - \sqrt{(1-CMF(a,b,c))(b-a)(b-c)}$ if

$\frac{c-a}{b-a} < CMF(a,b,c) \leq 1$. ReMOSST replaces $CMF(a,b,c)$ by a uniformly distributed distribution with values between 0 and 1.

Visualisation of results from the Monte Carlo simulation Figure 26 shows results of an example Monte Carlo simulation for one criteria and one portfolio. It shows mean, standard deviation, minimum and maximum values of the computed distribution.

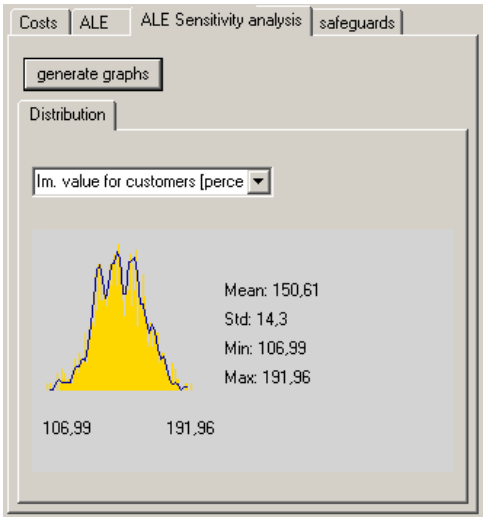


Figure 26: Results of a sensitivity analysis for one ReMOSST value criteria

8.4 Summary

This section presents the functions of the Odin ReMOSST brainstorming and portfolio analysis tool. It depicts a brainstorming step in five phases where each one comprised three steps: the brainstorming, the quantitative rating and the selection step. Next, it presents the analysis module that supports the selection of safeguard portfolios by the definition of bounds and the assertion of the robustness of the computed values by a Monte Carlo simulation visualised by a distribution chart.

9 Case study at uniforce Junior Enterprise Vienna

This chapter presents a case study where the Odin DSS using the ReMOSST plugin was used for the preparation, execution and analysis of a information security workshop. First in 9.1, it presents the company at which the workshop session was held and its characteristics relevant for information security risk analysis. Second, in 9.2, the design and realisation of the workshop will be presented. Finally in 9.3 the results of the workshop will be discussed and evaluated using the criteria defined above in 6.

9.1 Presentation of uniforce Junior Enterprise Vienna GmbH

Figure 27: uniforce logo

uniforce is a student-led company organized as an association. It defines itself as a junior enterprise. Put in perspective of the risk analysis, the following general aspects of this organisational form can be discerned:

- **High staff turnover:** JE members tend to limit their stay at uniforce to 3-4 semesters at most.
- **Importance of knowledge management:** without complete documentation of the work done, the JE would vanish in the case of a crisis.
- **External support is crucial:** the help of sponsors, partners and the nonsalaried advisory board gives the current team the image value it lacks due to lacking work experience when dealing with clients.

uniforce is in a very special situation and has developed a rather unique infrastructure since its incorporation in 1994.

- Firstly, it is located in the premises of the "Industriellenvereinigung" an institution lobbying for Austria's industry. It uses its phone and IT-infrastructure and access its offices through the concierge-supervised main entry.
- Secondly, the sponsors are renowned international consulting, attorney and tax advisory companies keen on getting positive publicity through their support for uniforce.

- Thirdly, a great amount of support is provided by university professors and alumni, cooperating in form of project work and the promotion of the junior enterprise idea.

These aspects shine a different light on the image of uniforce as a safe sand box enabling students to try out business practices. Regarding information security, these external environments should be taken into account - as they might be the source of specific risks.

The uniforce Balanced Scorecards Balanced Scorecards were introduced by Robert S. Kaplan and David Norton [KN92] as a method for measuring a company's activities in terms of its vision and strategies. In the context of the information security workshop, the formulation of its goals needs to take this performance measurement process into account, as it would otherwise ignore important aspects of this company's value chain. Each of this organisation's departments rates the quality and efficiency of its work with specific performance figures, presented in table 6.

Table 6: uniforce performance figures

Balanced Scorecard Goal	**Performance Figure**
QUALITY MANAGEMENT	
Adequate remuneration	Accuracy project workload estimation
High customer satisfaction	Feedback forms
Transparent and efficient business processes	Team interviews
Demanding projects	Ratio demanding / frustrating projects
FINANCE & CONTROLLING	
Financial independance	Budget vs. financial assets
Raise liquity	Financial assets
CRM	
Attract new customers	Number of new customers per year
Satisfying workload	Cumulated project values
	Successful bids
Improve image	Number of direct inquiries
HUMAN RESSOURCES MANAGEMENT	
Improve image	Num. of assessment center candidates
Enhance the network	Number of alumi actions
	Number of guest during events
High motivation	Team interviews
High know how	Skills number
High project experience	Number of project / team member
PUBLIC RELATIONS	
Improve image	Number of homepage visitors
IT AND SERVICES	
Improve image	Number of newsletter visitors

9.2 Design and realisation of the workshop

This section presents the steps taken before, during and after the workshop.

9.2.1 Preparation

In the first dialogs with the management of uniforce, it soon became clear that the analysis was only possible if it also included classical business continuity risks. It was decided to extend the analysis to these risks, even if they would not be covered by the ReMOSST risk analysis tool. Therefore, the ReMOSST model would cover the InfoSec risks whereas a classical risk analysis would deal with the risks that are not linked to InfoSec[159]. This would furthermore enable the comparison between the „classical“ risk analysis approach and the ReMOSST model using the requirements defined in 6. Afterwards, a questionnaire[160] was prepared and sent to all potential participants.

The next step was the gathering of data required by the risk analysis using following sources:

- Personal face-to-face discussions with the management
- Personal face-to-face discussions with IT experts
- Personal face-to-face discussions with selected key-users
- Simple questionnaire sent to alumni by email
- Short analysis of server log-file data
- Analysis of the „BSI Grundschutzhandbuch“ [Bun05]
- Questionnaire filled out by workshop participants

This data was structured and entered into the ReMOSST GDSS. Additionally a user account was created for each workshop participant. After setting the date of the workshop, a workshop description in form of a Microsoft Powerpoint presentation was prepared and sent to the participants.

The day of the workshop, the following technical items were prepared:

Room: A workshop room needs to be organised.

Food and beverages: Because of the projected workshop length of three hours, food and beverages had to be prepared.

[159] See Gotaishi [Got04].
[160] See A.

Server: A Odin ReMOSST Server and a MS SQL 2003 database had to be installed and configured.

Video projector: The Odin ReMOSST server was projected onto a wall using a video projector.

Ethernet network: Each ReMOSST client neeed to be linked to the server using a dedicated ethernet network.

Clients: For each client, the Odin ReMOSST software had to be installed and configured. Moreover, specific network configurations were deactivated, especially proxy, firewall and other network interfaces.

Voice recorder: A voice recorder was helpful to document the flow of the workshop and to analyse the major problems and improvements during the wrap-up phase.

9.2.2 Execution

The start of the workshop depends on following prerequisites, which in this case caused the workshop to be delayed[161]:

- All team members need to be present.
- The technical infrastructure must be set up and working.

As an introduction, the expectations of the participants are gathered and written on a flipchart. Next, a Microsoft Powerpoint presentation presents the goals, focus and steps of the workshop. In a first step, a classical risk analysis including the following steps covers general business continuity risks, not only related to information security:

- Definition of main business functions and criteria for their continuity
- Brainstorming of the main risks threatening continuity and estimation of the impacts and likelihood
- Brainstorming of measures that could be taken to limit these risks, estimation of their costs
- Agreement on responsibilities and on the implementation deadline.

During each of the presented steps, results are written on a flip chart. Finally the main findings of the workshop are summarised in the group and a feedback round completes the first RA.

[161] Half of the team members were half an hour late and the laptop computers required for the workshop had unanticipated configuration issues.

As introduction to the second RA - using ReMOSST - a second Microsoft Powerpoint presentation describes the agenda, the most important relevant RA quantification theories and the main steps. The workshop comprises the steps described in 8.2.

The ReMOSST RA is rounded off by a summary and a feedback round. Alternatively, the portfolio analysis tool can be presented and a quick overview of the outcome can be provided to interested participants.

9.2.3 Wrap-up phase

The wrap-up phase comprises following steps:

- The post-processing and evaluation of the workshop data stored in ReMOSST
- The distribution of questionnaires for the evaluation of the workshop[162]
- The analysis of the questionnaire's results
- The writing of a final report

9.3 Analysis of the workshop's results

After the completion of the workshop, a report about the knowledge gathered during the workshop was written[163] and the workshop was evaluated using the feedback of the participants, voiced through a questionnaire[164]. This section analyses the feedback of the participants and tries to validate the ReMOSST workshop against the requirements defined in 6 .

The workshop participants background and perspective on information security:
The 5 participants' backgrounds at the workshop range from the finance department to IT and services[165]. Most participants were highly computer literate[166] and had backgound knowledge about information security[167]. The time taken for preparation was therefore less than three hours.

[162] A questionnaire for the evaluation of the workshop can be found in B.
[163] The business continuity report can be found in C.
[164] See B for the evaluation questionnaire used during the case study.
[165] All three employees of the IT department were present, one member of the board and an employee of the finance department.
[166] All participants could use every IT service available, three could even configure them.
[167] Two out of four had above average knowledge about information security.

The importance of information security in the areas of internal work, external relations and projects was equally asserted. Its role was mainly seen as defined by the Libertian design ideal[168], thus helping „individuals to overcome physical, temporal and organisational limitations, thus being able to work efficiently and in a focused way.“. Regarding the dimension that should be quantified, participants rated „monetary costs“, „maintenance work“ and „user acceptance“ best and did not express explicit support for the options „nonsalaried work“ and „ethical and privacy costs“.

9.3.1 Evaluation of the workshop

This section presents the evaluation of the workshop using the requirements defined in 6.1.

Management orientation

The presence of a member of the board and the support of the management by providing information and by allocating resources[169] to the project were prerequisites for the organisation of the workshop. Due to the explicit focus on metrics and goals which are compatible to the existing performance management systems, the benefit of the workshop could be easily explained and was well understood by all participants.

Completeness of the analysis

The InfoSec RA alternatives were prepared by the methods described above, which ensured that nearly all could be found. Moreover the suggestions by respondents in the preparation questionnaire were all included in the risk analysis. Whereas omissions seemed highly unlikely, criticism arose because most participants would have preferred a lower number of alternatives to concentrate on[170].

Scalability of the analysis

Because of the quantity of alternatives identified during the preparation, the workshop participants tried to divide the work into packages. Participants with low knowledge about their assigned package tried to communicate to their neighbours with the aim of procuring the information required to contribute to the workshop. This lead to fewer ratings per alternative, showing that there is an individual cognitive limit for the number of processed alternatives. Therefore it can be concluded that more alternatives require a greater number

[168] See 4.1 for a description of major design ideals.
[169] This included time of employees, the technical infrastructure and the room where the workshop took place.
[170] This number could range from 10 to 15 items per workshop phase.

of participants who should focus their contribution to certain domains of the analysis, depending on their knowledge. It should be noted that the building of expert groups could also be observed during the paper-based business continuity RA.

Comprehensibility of the process

According to their feedback, the workshop was well understood by the participants. Their ratings concerning understandability and problem clarification were above average. However, ratings were a bit lower regarding the comprehensiveness of the workshop group decision process steps, the multiple criteria ratings and the qualitative ratings procedure. In contrast the hands-on paper-based business continuity RA appeared more workable and understandable.

Time and cost efficiency

The response from the workshop participants was strongly related to their disciplinary background. Whereas the staff from the IT-department responded in a highly approving manner - stating that the effort was worth the outcome - one participant with a non-technical background and with little knowledge about information security thought that the workshop was too time-consuming and should not be repeated. In a personal discussion, the respondent felt that the outcome of the paper-based business continuity RA was superior in quality and quantity than the ReMOSST-supported InfoSec RA and took less time.

9.3.2 Evaluation of the ReMOSST brainstorming module

This section presents the evaluation of the ReMOSST brainstorming module using the requirements defined in 6.2.

Mitigation of group decision drawbacks

The main group decision drawbacks were effectively avoided by the use of the ReMOSST brainstorming module: these included group polarisation, efficiency losses due to cumbersome communication and the group think phenomenon. However, during the paper-based RA, performed before the ReMOSST-supported InfoSec RA these problems did not become apparent, leaving the claim that the use of the ReMOSST brainstorming module helps to cope with group decision drawbacks unverified.

Fast convergence of decisions with heterogeneous groups

Decisions were reached in very short time periods and did not initiate arguments between

participants. Nor were time-consuming discussions observable during the business continuity RA. This was largely due to the fact that the attention of the participants was very fixed on getting the quantitative ratings right - leaving no room for necessary communication. During the selection step, participants talked about their ratings, resulting in one iteration for the correction of a rating value. Finally, each of the 5 ReMOSST steps were completed in less than 15 minutes.

Comprehensibility and user friendliness

The users of the brainstorming module responded with above average grades for the rating of ReMOSST brainstorming module's user friendliness. Nevertheless, it was noted that more complex interactions were found to be less user friendly, which may be a sign that the user interface could be improved.

Short preparation time for the technical infrastructure

This requirement was not met during the case study, as the available infrastructure proved to interfere with the ReMOSST workshop system. The following problems occurred:

- Laptop clients could not connect to the WLAN network of the company. It was thus necessary to switch to cables-based Ethernet LAN.
- The company Ethernet LAN infrastructure prevented the .NET Remoting connection between three clients and the server. A separate network infrastructure using an autarkic switch device had to be set up.
- The configuration of the clients prevented Odin .NET Remoting clients to connect to the Odin server, mainly because of proxy server settings set in the Internet browser configuration dialog.
- Due to a very sunny day and a under powered video projector, the projection of the Powerpoint presentations and of the Odin brainstorming module were difficult to follow. This lead to much confusion and laborious communication between the moderator and the workshop participants.

Effective and efficient workshop work-flow

The effectiveness of the workshop workflow was without question lowered by the unanticipated technical difficulties, the great number of alternatives, the perceived time constraints and the pressures that therefore resulted. However, due to the division of labour which helped in the completion of all steps and the completeness of the ratings, the collected data reflected satisfactorily the participants' view of information security issues relevant for the company. Even if the post-processing of the collected data proved to be very

time-consuming and objectively reduced the efficiency of the workshop, the participants - obviously not concerned with this work - were satisfied with its efficiency.

Multi-criteria ratings

This requirement was met and the functionality of multi-criteria ratings was used by all participants during the workshop. Multi criteria ratings were used in risk and safeguard rating and provided precious data for the selection of an optimal portfolio. When compared with the paper-based business continuity RA, the ReMOSST-powered RA collected more multi-criteria data and lead therefore to a more differentiated view of risks.

9.3.3 Evaluation of the portfolio selection module

Pareto optimisation The ReMOSST processing module implements an algorithm generating all portfolios by combination of safeguards, computes the summed costs/ALE values and compares them in order to select the ones that are Pareto-optimal. Optionally, the Pareto optimisation uses a Monte Carlo simulation to determine whether the portfolio values are significantly distant[171].

Nevertheless the quality of this step's output depends highly on the data provided by the workshop participants. Moreover, the Monte Carlo simulation should be limited to a few runs, as it takes a rather long time to complete.

Criteria value range definition By setting limits to the valid criteria values, the analysis can be restricted in order to filter portfolios that are acceptable for the decision maker. The implementation of this functionality requires user input in the form of integer numbers, which might by perceived as cumbersome. However, the criteria value range data can be saved by copy-and-pasting the spreadsheet table into an external software, which is in turn helpful for the documentation of the workshop.

Sensitivity analysis The implemented sensitivity analysis computes ALE values with random risk annual rate of occurrence values[172]. It provides information about the minimum, maximum, mean and variance values and visualizes the distribution of the simulated distribution. This functionality is helpful for a detailed analysis of portfolios ALE values and their robustness, but requires a lot of time for computation. Moreover it is complex to handle and conclusions are difficult to draw on its' results.

[171] This helps determining whether a given portfolio dominates another one.

[172] The distribution of the random risk ARO values follows a triangular distribution.

9.4 Summary

This section presents the preparation, execution and evaluation of a field study at uniforce junior enterprise GmbH. in Vienna, Austria. It first presents the specificites of this company, its performance evaluation system and its business goals. The importance of linking these elements to information security management is discussed. Next, it presents the main requirements for the ReMOSST workshop including the participants, technical infrastructure and its date. It then describes how it was held, how its results were handled afterwards and presents the evaluation of the ReMOSST workshop and the ReMOSST brainstorming and portfolio selection tools.

The main educational aspects included the difficulty of finding participants with a non-technical background, the importance of eliminating technical hindrances in due time, the difficult handling and understanding of complex interactions[173] by the users of the ReMOSST DSS. The proposed DSS-supported information security risk analysis is certainly very demanding in terms of cognitive skills, knowledge about information security and the struggle in dealing pragmatically with quantification.

[173]The main difficulties emerged with the quantitative rating of items which depended on aggregated values, including safeguards and safeguard dependencies. This opens opportunities for improvements in the graphical user interface and visualisation.

10 Conclusions

This work is structured in three units. First, it discusses the main related work including the fields of information security management, the approaches to quantify items discussed during a information security risk analysis, group decisions and methods for the ranking of alternatives in group decisions. Second, it presents the main requirements for a group decision workshop for a „holistic“ information security risk analysis and for the ReMOSST DSS tools. Third, it presents the developed ReMOSST workshop and ReMOSST DSS and a case study where it was implemented and evaluated.

The main research questions to be treated include the issue of quantification, the difficulty of dealing with uncertain data in information security and the challenge of making group decisions efficient by the use of a GDSS.

The main findings of this work include the importance of management support, the necessity of the integration of the information security management process and existing performance measurement systems and the imperative of a multi-disciplinary approach focusing content-wise on a risk analysis unbiased towards technical solutions and process-wise on the participation of experts/stakeholders of all relevant fields.

This has lead to various new issues to be explored in further research: first, incentives to participate need to be properly communicated to all relevant stakeholders and complex risk analysis steps should be redesigned to be simpler to complete. Moreover the computation of portfolio ALE and cost values - currently implemented using simple, linear aggregations - might require further examination regarding the aggregation of user ratings and the computation of risk likelihoods[174]. Finally, the modeling of safeguards investments should cover more complex decision making parameters including the sequencing of the implementation of safeguards using a multiple period model.

[174]For instance, the ReMOSST model does not deal with the issue of correlated risks explicitly, which could lead to higher computed ALE values.

References

[A-S04] A-SIT: Zentrum fÃ¼r sichere Informationstechnologie - Austria, *Österreichisches IT-Sicherheitshandbuch, Teil 1: IT-Sicherheitsmanagement*, Bundeskanzleramt Oesterreich - IKT-Stabsstelle des Bundes, Nov 2004.

[AFM00] William A. Arbaugh, William L. Fithen, and John McHugh, *Windows of Vulnerability: A Case Study Analysis*, Computer **33** (2000), no. 12, pp. 52–59.

[AH03] Farnaz Akhavi and Caroline Hayes, *A Comparison of Two Multi-Criteria Decision-Making Techniques*, IEEE International Conference on Systems, Man and Cybernetics **1** (2003), 956 – 961.

[ALRL04] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, *Basic Concepts and Taxonomy of Dependable and Secure Computing*, Dependable and Secure Computing, IEEE Transactions on **1** (2004), no. 1, pp. 11–33.

[Ame00] American College of Physicians' Effective Clinical Practice, *Primer on Cost-Effectiveness Analysis*, September/October 2000.

[And01] Ross Anderson, *Why Information Security is Hard - An Economic Perspective*, ACSAC '01: Proceedings of the 17th Annual Computer Security Applications Conference (Washington, DC, USA), IEEE Computer Society, Jan 2001, aus Schechter04.

[Bae94] Rudolf Baer, *Informatik-Sicherheit, Konzept und Vorgehen*, Fachpresse Goldach ed., vol. 13, BSG Unternehmensberatung St. Gallen, München Wien, 1994.

[BEvW91] Katrin Borcherding, Thomas Eppel, and Detlof von Winterfeldt, *Comparison of Weighting Judgements in Multiattribute Utility Measurement*, Management Science **37** (1991), no. 12, 1603–1619.

[BF02] Shawn Butler and Paul Fischbeck, *Multi-Attribute Analysis For Incorporating Nontechnical Attributes in Multi-attribute Analysis for Security*, Proceedings from Symposium on Requirements Engineering for Information Seurity (SREIS), 2002.

[BH03] Bhagyavati and Glenn Hicks, *A basic security plan for a generic organization*, J. Comput. Small Coll. **19** (2003), no. 1, pp. 248–256.

[BHKS05] Prof. Dr. Stefan Biffl, Matthias Heindl, Christoph Kozarits, and Katja Schmidt, *Skriptum zur Lehrveranstaltung Risiko Management*, 2005.

[Bjo01] Fredrik Bjoerck, *Security Scandinavian Style*, Master's thesis, Stockholm University - Royal Institute of Technology, 2001.

[BK92] S. P. Benett and M. P. Kailay, *An Application of Qualitative Risk Analysis to Computer Security in the Commercial Sector*, Proceedings of the Eighth ACM Annual Computer Security Applications conference **1** (1992), 64–73.

[BMG01] Bob Blakley, Ellen McDermott, and Dan Geer, *Information Security Is Information Risk Management*, Proceedings of the 2001 workshop on New security paradigms, ACM Press, 2001, pp. 97 – 104.

[Bre00] Dr. David Brewer, *Risk Assessment Models and Evolving Approaches*, IAAC workshop, July 2000, URL: http://www.gammassl.co.uk/topics/IAAC.htm (22 March 2002).

[Bun05] Bundesamt für Sicherheit in der Informationstechnik, *IT-Grundschutzhandbuch: Stand 2005*, 2005.

[But02] Shawn Butler, *Security Attribute Evaluation Method: A Cost-Benefit Approach*, International Conference on Software Engineering (ICSE) Proceedings, 2002.

[BZ00] Rudolf Baer and Pius Zaengerle, *Wie misst man IT-Sicherheit?*, HMD - Praxis Wirtschaftsinform. **216** (2000), pp. 67–77.

[Cla95] R. Clarke, *Computer matching by government agencies: The failure of cost/benefit analysis as a control mechanism*, Information Infrastructure and Policy **4** (1995), no. 1, pp. 29–65.

[CMBR04] Huseyin Cavusoglu, Mishra. Birendra, and Srinivasan Raghunathan, *A model for evaluating IT security investments*, Commun. ACM **47** (2004), no. 7, pp. 87–92.

[Com03] Committee on National Security Systems, *National Information Assurance (IA) Glossary*, 2003.

[Deb90] C.J. Debeljak, *Integration of surrogate worth trade-off method in AHP*, Socio Economic Planning **20** (1990), pp. 375–385.

[DH04] John D'Arcy and Anat Hovav, *The Role of Individual Characteristics on the Effectiveness of IS Security Countermeasures*, Proceedings of

the Tenth Americas Conference on Information Systems, New York, New York, 2004.

[Dhi01] Gurpreet Dhillon, *Challenges and principles in managing information security in the new millennium*, 2001.

[DT01] Gurpreet Dhillon and Gholamreza Torkzadeh, *Value-Focused Assessment of Information System Security in Organizations.*, ICIS (Veda C. Storey, Sumit Sarkar, and Janice I. DeGross, eds.), Association for Information Systems, 2001, pp. 561–566.

[Dye90] J. S. Dyer, *Remarks on the analytic hierarchy process*, Manage. Sci. **36** (1990), no. 3, pp. 249–258.

[EB94] W. Edwards and F.H. Barron, *SMARTS and SMARTER: Improved simple methods for multiattribute utility measurement*, Organizational Behavior and Human Decision Processes **60** (1994), no. 3, p. 306.

[Fin96a] Thomas Finne, *A DSS for Information Security Analysis: Computer Support in a Company's Risk Management*, Systems, Man, and Cybernetics, 1996., IEEE International Conference, 1996, booktitle noch nicht ganz irchtig.

[Fin96b] _____, *CBISA - a DSS for Analysing a Company's Information Security: A Tool for Decreasing Uncertainty*, Technical Report TUCS-TR-29, Turku Centre for Computer Science, Finland, 1996.

[Fin96c] _____, *Computer Support for Information Security Analysis in a Small Business Environment*, Technical Report TUCS-TR-30, Turku Centre for Computer Science, Finland, Juni 1996.

[Fin97] _____, *Information Security implemented in: the theory of stock market efficiency, Markovitz's Portfolio Theory and Porter's Value Chain*, Computer & Security **16** (1997), pp. 469–479.

[Fin98a] _____, *A conceptual framework for information security management*, Computers & Security **17** (1998), no. 4, pp. 303–307.

[Fin98b] _____, *The Three Categories of Decision-Making and Information Security*, Computers & Security **17** (1998), pp. 397–405.

[Fin00] _____, *Information Systems Risk Management: Key Concepts and Business Processes*, Computers & Security **19** (2000), no. 3, pp. 234–242.

[FNES03] Fariborz Farahmand, Shamkant B. Navathe, Philip H. Enslow, and Gunter P. Sharp, *Managing vulnerabilities of information systems to security incidents*, ICEC '03: Proceedings of the 5th international conference on Electronic commerce, ACM Press, 2003, pp. pp. 348–354.

[Got04] Masahito Gotaishi, *Business Continuity Planning beyond ISO17799*, Tech. report, SANS Institute, 2004.

[GvS05] Mariana Gerber and Rossouw von Solms, *Management of risk in the information age*, Computers & Security **24** (2005), no. 1, pp. 16–30.

[HALMT75] Harold A. Linstone and Murray Turoff, *The Delphi Method: Techniques and Applications*, Addison-Wesley Publishing, 1975.

[Hoo00] Kevin Soo Hoo, *How Much Is Enough? A Risk-Management Approach to Computer Security*, Ph.D. thesis, Stanford University, June 2000.

[Ihe04] Charles Iheagwara, *The effect of intrusion detection management methods on the return on investment*, Computers & Security **23** (2004), no. 3, pp. 213–228.

[Ira99] Zahir Irani, *IT/IS Investment Justification : An Interpretivist Case Study*, Proceedings of the 32nd Hawaii International Conference on System Sciences, 1999.

[IT 04] IT Governance Institute, *The ING Case Study*, URL: http://www.itgi.org/ (June 15, 2006), 2004.

[Jan72] Irving Lester Janis, *Victims of groupthink: A psychological study of foreign-policy decisions and fiascoes*, Houghton, Mifflin, 1972, in Martirossian 2001.

[Kam82] RD Kamenetzky, *The relationship between the analytic hierarchy process and the additive value function*, Decision Sciences **13** (1982), pp. 702–713.

[Ker97] Gregory E. Kersten, *Support for Group Decisions and Negotiations An Overview*, INR04/97 **1** (1997), 15.

[KN92] R.S. Kaplan and DP Norton, *The balanced scorecard–measures that drive performance.*, Harvard business review (Harvard bus. rev.) **70** (1992), no. 1, 71–90.

[Kol04] Ella Kolkowska, *Values in managing of IS security - The Ph.D theses project*, Proceedings of the 27rd Information System Research Seminar in Scandinavia (IRIS 27) **1** (2004), pp. 1–20.

[KR76] Ralph L. Keeney and Howard Raiffa, *Decisions with multiple objectives: Preferences and value tradeoffs*, Wiley, 1976.

[KTTW03] Atreyi Kankanhalli, Hock-Hai Teo, Bernard C.Y. Tan, and Kwok-Kee Wei, *An integrative study of information systems security effectiveness*, International Journal of Information Management **23** (2003), pp. 139–154.

[Lan01] Carl E. Landwehr, *Computer security*, International Journal of Information Security **1** (2001), no. 1, pp. 3–13.

[Mak04] Marek Makowski, *Multi-objective Decision Support Including Sensitivity Analysis*, UNESCO-EOLSS Joint Committee, Encyclopedia of Life Support Systems, Eolss Publishers, 2004, http://www.eolss.net, article no 001-373 (4.20.4.3).

[Mar01] Jasmine Martirossian, *Decision Making in Communities: Why Groups of Smart People Sometimes Make Bad Decisions*, Community Associations Press A Division of Community Associations Institute, 2001.

[Mer03] Rebecca T. Mercuri, *Analyzing security costs*, Commun. ACM **46** (2003), no. 6, pp. 15–18.

[MMGAFJNDG02] Manuel Mora, Guisseppi A. Forgionne, and Jatinder N. D. Gupta, *Decision Making Support Systems: Achievements, Trends and Challenges for the New Decade*, Idea Group Publishing, 2002.

[MS01] Kenneth E. Murphy and Steven John Simon, *Using Cost Benefit Analysis for Enterprise Resource Planning Project Evaluation: A Case for Including Intangibles*, Proceedings of the 34th Hawaii International Conference on System Sciences, 2001.

[Mus99] Jyri Mustajoki, *Web-HIPRE - A Multiattribute Decision Support System on the Internet*, Masters Thesis, 1999.

[Nat] National Information Center on Health Services Research and Health Care Technology (NICHSR), *HTA 101: Glossary*, URL: http://www.nlm.nih.gov/nichsr/hta101/ta101014.html (April 29, 2006).

[Nic02] Arthur Nichols, *A Perspective on Threats in the Risk Analysis Process*, Tech. report, SANS Institute, 2002.

[NIS02] NIST, *Risk Management Guide for Information Technology Systems*, NIST, July 2002.

[NM05] Thomas Neubauer and Thomas Mikscha, *Odin - A Tool for distributed multiobjective decision support*, Tech. Report TR-TN-0105, IFS, 2005.

[Noo98] N. Noorderhaven, *Strategic Decision Making*, Addison-Wesley Publishing Company Inc., 1998, in: Mustajoki 1999.

[Nun97] J.F. Nunamaker, *Future research in group support systems: needs, some questions and possible directions*, Int. J. Human-Computer Studies **47** (1997), pp. 357–385, in: Mustajoki [Mustajoki1999, 22].

[Pav99] Zareer Pavri, *Valuation of Intellectual Property Assets: The Foundation for Risk Management and Financing.*, Tech. report, PricewaterhouseCoopers., 1999.

[PCCW93] Mark C. Paulk, Bill Curtis, Mary Beth Chrissis, and Charles Weber, *Capability Maturity Model for Software, Version 1.1*, Tech. Report CMU/SEI-93-TR-24, Software Engineering Institute, February 1993, DTIC Number ADA263403.

[PD05] Preiß and Distelberger, *Softwareunterstützung für Workshops im Rahmen von Analyse Methoden*, Bakkalaureatsarbeit, 2005.

[Pel04] Thomas R Peltier, *Risk Analysis and Risk Management*, Information Systems Security **13** (2004), no. 4, p. 44.

[Por85] Michael E Porter, *Competitive Advantage, Creating and Sustaining Superior Performance*, The Free Press. NewYork, 1985.

[Pur04] Steve A. Purser, *Improving the ROI of the security management process*, Computers & Security **23** (2004), no. 7, pp. 542–546.

[RD04] Thomas Rauschen and Georg Disterer, *Identifikation und Analyse von Risiken im IT-Bereich*, HMD - Praxis Wirtschaftsinformatik **236** (2004), pp. 19–32.

[REHN99] G. Rudinger, J. Espey, H. Holte, and H. Neuf, *Mehrseitige Sicherheit in der Kommunikationstechnik, Bd. 2 Erwartung, Akzeptanz, Nutzung*, ch. Der menschliche Umgang mit Unsicherheit, Ungewißheit und

(technischen) Risiken aus psychologischer Sicht, pp. S. 69–97, Bonn: Addison-Wesley, 1999.

[Roe03] Susanne Roehrig, *Using Process Models to Analyse IT Security Requirements*, Ph.D. thesis, Wirtschaftswissenschaftliche Fakultäet der Universität Zürich, 2003.

[Roy91] Bernard Roy, *The outranking approach and the foundations of electre methods*, Theory and Decision **31** (1991), no. 1, 49–73.

[Saa94] Thomas L Saaty, *How to Make a Decision: The Analytic Hierarchy Process*, Interfaces **24** (1994), no. 6, pp. 19–44.

[Sch92] Edgar H Schein, *Organizational Culture and Leadership*, Jossey-Bass, 1992.

[Sch04] Stuart Schechter, *Computer Security Strength & Risk: A Quantitative Approach*, Master's thesis, Harvard University, May 2004, p. 156.

[Sip00] Mikko Siponen, *A conceptual foundation for organizational information security awareness*, Information Management & Computer Security **8** (2000), no. 1, 31–41.

[Smi93] Martin Smith, *Commonsense Computer Security, your practical guide to information security*, McGraw-Hill Book Company, 1993, from: Finne 1998, 304.

[SS02] Christian Stummer and Christine Strauss, *Multiobjective Decision Support In It-Risk Management*, International Journal of Information Technology & Decision Making **1** (2002), no. 2, pp. 251–268.

[SS04a] S.W. Smith and Eugene H. Spafford, *Grand Challenges in Information Security: Process and Output*, IEEE Security & Privacy **2** (2004), pp. 69–71.

[SS04b] Basie von Solms and Rossouw von Solms, *The 10 deadly sins of information security management*, Computers & Security **23** (2004), no. 5, pp. 371–376.

[Ste02] Dirk Stelzer, *Risikoanalysen als Hilfsmittel zur Entwicklung von Sicherheitskonzepten in der Informationsverarbeitung*, Hermann Locarek-Junge (Hrsg.), 2002.

[Sve05] Anders Svensson, *Analysing Information Systems Security*, Proceedings of the 27rd Information System Research Seminar in Scandinavia (IRIS 27), 2005.

[Tan02] Ding Tan, *Quantitative Risk Analysis Step-By-Step*, Tech. report, SANS Institute, 2002.

[Tew04] Claudia Tewald, *Risikomanagement mit Hilfe der Erfolgsfaktoren-basierten Balanced Scorecard für die Informationsverarbeitung*, Information Management & Consulting **19** (2004), no. 1, pp. 80–83.

[Thi04] Christoph Thiel, *Ein Reifegradmodell für das IT-Sicherheitsmanagement*, HMD - Praxis Wirtschaftsinform. **236** (2004), pp. 52–58.

[Tom03] Emma L. Tompkins, *Using Stakeholders Preferences In Multi-Attribute Decision Making: Elicitation and Aggregation Issues.*, Tech. report, Centre for Social and Economic Research on the Global Environment and The Tyndall Centre for Climate Change Research, University of East Anglia, 2003, CSERGE working paper ECM 03-13.

[Urb02] Carol A. Urban, *Security Risk Management*, presentation at AZSAGE, September 11th 2002, URL: http://www.azsage.org/present/091102/RiskMgmt.ppt (29.04.2006).

[vS01] Basie von Solms, *Information Security - A Multidimensional Discipline*, Computers & Security **20** (2001), no. 6, pp. 504–508.

[WD05] Elizabeth F.R. White and Gurpreet Dhillon, *Synthesizing Information System Design Ideals to Overcome Developmental Duality in Securing Information Systems*, Proceedings of the 38th Hawaii International Conference on System Sciences, 2005.

[Yaz02] Zeki Yazar, *A qualitative risk analysis and management tool - CRAMM*, Tech. report, SANS Institute, 2002.

[YRL92] C.S. Yap, K.S. Raman, and C.M. Leong, *Methods for information system project selection: an experimental study of AHP and SMART*, System Sciences, 1992. Proceedings of the Twenty-Fifth Hawaii International Conference on, vol. 3, 1992, pp. 578–589.

[Zuc02] Albin Zuccato, *Towards a systemic-holistic Security Management*, Ph.D. thesis, Karlstad Unviersity Studies, Karlstad, 2002.

List of Figures

List of Tables

List of Algorithms

A A questionnaire for the workshop's preparation

A.1 The personal information security knowledge level

Personal information:

Name: .....

Position: .....

How would you describe your knowledge of your company's IT systems?

[ ] I can use the most important services (email, file repository)

[ ] I can use all services

[ ] I can use and configure all services

How much do you know about information security management?

[ ] 1 - poor

[ ] 2

[ ] 3 - average

[ ] 4

[ ] 5 - high

How much time did you reserve for the preparation of this workshop session?

[ ] less than an hour

[ ] less than three hours

[ ] less than five hours

[ ] more

A.2 The perceived role of information security in the organisation

How would you describe the state of information security management in your company?

[ ] blind faith (carefree working, goal orientation, ignorance)

[ ] ad-hoc efforts (short-term solutions, workarounds, „enemy is external“)

[ ] security policies (existence and realisation of security policies, security awareness, systematisation)

[ ] evolutionary (security management and the organisation are evolving in unisono)

How important is information security for:

- the internal work in your department? __ (1-5)
- the external relations? __ (1-5)
- the acquisition and delivery of projects? __ (1-5)

In your eyes, what is the role of information technology in general and security in particular?

- Information systems are means to reach certain pre-defined objectives and should be efficient and reliable __ (1-5)
- Information systems should strengthen the role of „institutions“ (providing adequate information, power and visibility) and therefore enable conflictuous point of views and negotiations resulting in higher quality __ (1-5)
- Information systems and their security should help individuals to overcome physical, temporal and organisational limitations, thus being able to work efficiently and in a focused way. __ (1-5)
- Information Systems should be available and intelligible to all stakeholders, their design should not be imposed and closely tied to the organisation. __ (1-5)
- Other role: .....
  ..... __ (1-5)

A.3 The critical success factors for information security

Which of the following critical success factory could oppose the successful implementation of information security measures in your company and should therefore be considered:

- monetary costs __ (1-5)
- nonsalaried work __ (1-5)
- maintenance work __ (1-5)
- user acceptance __ (1-5)
- ethical and privacy costs __ (1-5)

- other: ..... __ (1-5)

Please identify the most commonly used information assets (information systems, folders, partners, employees, etc.) that - if lost - would lead to losses or endanger business continuity:

....

....

Please identify the most dangerous threats to information that would lead to losses or endanger business continuity:

....

....

Please identify safeguards or security measures that would reduce the threats named above:

....

....

A.4 Comments

.....

.....

.....

.....

.....

.....

B A questionnaire for the workshop's evaluation

B.1 General Information

Personal information:

Name: .....

Position: .....

Did you stay during the whole duration of the workshop?

[ ] Yes

[ ] No, but at least 75 % of the time

[ ] No, but at least 50 % of the time

[ ] No, but at least 25 % of the time

How much could you contribute to the workshop - in comparison with the other participants?

[ ] More than the other participants

[ ] At least as much as the other participants

[ ] Less than the other participants

Why?

.....

.....

.....

B.2 Comprehensability and problem clarification in the group

Please rate the comprehensabilty of the following items tasks and items:

- the workshop group decision process, its structure (phases, steps): ___ (1-5)
- the risk analysis model: ___ (1-5)
- the formulation of the items of consideration: ___ (1-5)S]
- the multi-criteria ratings: ___ (1-5)

- the qualitative rating procedure (goals, assets and vulnerabilities) using multiple criteria: ___ (1-5)
- the quantitative rating procedure (threats, risks and safeguards): ___ (1-5)

Would you like to further comment the comprehensibility of any aspects of the workshop process?

.....

.....

How did the workshop process help you to understand the problem and to clarify the main information security risks and tasks?

[ ] It provided me new unknown insights into the risks my company is facing

[ ] It showed me how - from now on - I can contribute to the information security of my company

[ ] It enabled me to take an active part in the decision process: I could interactively influence the outcome of the process and contribute actively to the decision making.

B.3 Completeness of the risk analysis

How do you judge the completeness of the risk analysis, in particular following items:

- Information security goals: ___ (1-5)
- Assets: ___ (1-5)
- Vulnerabilities: ___ (1-5)
- Threats: ___ (1-5)
- Risks: ___ (1-5)
- Safeguards: ___ (1-5)

If you rated one or more items below 3, please provide some information about what has been left out:

.....

.....

B.4 Contentment with the results and the process

How do you judge the quality of the results of:

- the quantitative multi-criteria risk analysis
  - the creation of links between assets, vulnerabilities and threats: ___ (1-5)
  - the rating of risks' annualized rate of occurrence: ___ (1-5)
  - the rating of risks' multi-criteria impact: ___ (1-5)
  - the selection of risks: ___ (1-5)
- the safeguard brainstorming and quantification
  - the definition of safeguards: ___ (1-5)
  - the rating of safeguards' ability to reduce threats' annualized risk of occurrence: ___ (1-5)
  - the rating of safeguards' ability to reduce risks' impacts: ___ (1-5)

If you rated one or more items below 3, please provide some information about what has could have been done better:

.....

.....

How would you rate the „results to group time requirement ratio“ of the ReMOSST workshop?

[ ] the time required by the workshop was fully justified by the results

[ ] the results could have been also obtained with less participants

[ ] more and/or better results could have been reached with less participants

Do you accept the outcome of the process?

[ ] Yes fully.

[ ] Partly, it should not be repeated, reason: _____

[ ] Partly, it should be repeated, reason: _____

[ ] No, reason: _____

If you like, you can describe what lead to your (dis-)contentment with the results of the workshop process:

.....

.....

.....

B.5 User friendliness

Please rate the user friendliness of the following interactions of the ReMOSST Brainstorming module:

- the definition of goals, assets, vulnerabilities, threats and safeguards using trees: ___ (1-5)
- the rating of goals, assets, vulnerabilities and threats: ___ (1-5)
- the definition of risks by creating links between assets, vulnerabilities and threats: ___ (1-5)
- the rating of risks (annualized rate of occurrence, multi-criteria impact): ___ (1-5)
- the rating of safeguards regarding its' reduction of the annualized rate of occurrence: ___ (1-5)
- the rating of safeguards regarding its' reduction of the multi-criteria impact: ___ (1-5)

If you like, you can comment other usability aspects that might be improved:

.....

.....

.....

B.6 Comments

.....

.....

.....

.....

C Business continuity report

C.1 Project description

C.1.1 Project initiation context

This document was created in the course of the field study of Michael Schramel's master's thesis. It presents the results of the risk analysis workshop covering business continuity risks in a paper-based risk analysis (RA) and information security risks in a RA supported by the ReMOSST DSS.

The following events from the near past mark the importance of this document as a measure to avoid such incidents in the future:

2006 - April: Corporate tax supplementary payment
Because of a bookkeeping mistake at the end of the tax period 2004, expenses were not taken into account, thus resulting in record profits in 2004 and considerable losses in 2005. This mistake was not identified during bilancing and resulted in additional claims by the tax office in 2006. Moreover, three times higher advance payments were calculated, ripping a large (temporary) hole in the liquidity predictions of the finance department FCQM. The decided budget was cut down and important investments had to be postponed.

2006 - April: Notebook theft and loss of company data
While a co-worker was out shopping, her flat was burglarised and her private notebook stolen. As she was a long-time member of the board, an enormous amount of important and critical company data was lost and made available to criminals. The cost of this incidents were increased by the fact that she did not save this data on the company's file server resulting in the total loss of this data.

2006 - February to May: Workstation hard disk failures
During this short lapse of time, three out of seven office workstations had hardware failures linked to the power supply adopter (Netzteil) and to the hard disk, resulting in data loss in an unknown amount and in business process disruption because of lost software and project data. The causes of these incidents are subject to controversy: some argue that not powering off the PCs cause them to fail, others argue that power outages and voltage fluctuations put the material under stress and lead to earlier failures. However, these incidents - combined with lax policies on saving company data on the file server - caused considerable costs incurred by the lost data, the business process interruption and the recovery actions.

2006 - March: Intrusion by a former employee

An alumni was caught sitting at a workstation before official office hours began. The purpose of this intrusion is unknown and the damage - if any - cannot be assessed. Anyhow this incident is to be taken seriously, as it shows that more or less any external individual could do the same.

2005 - June: Server hard-disk crash - loss of all file-server data and emails

The hard disk of the one-year old server crashed, leading to major data loss and business disruption for one and a half weeks. If backups would have been up-to-date and if a recovery plan had been in place, the loss and the down time could have been limited to a more acceptable level.

2005 - May: No response regarding the year closing by the auditors

The auditors are uniforce partners and support the company by checking the year closing. Unfortunately, responses to inquiries take impressively long and this was the reason for flaws in the annual tax declarations.

2005 - January: Threat of annulment of the private limited company (GmbH.) by the commercial court

During the past three years, the board did not send the annual accounts (Jahresabschluss) to the commercial court. This lead to a letter announcing that the private limited company was bound to be annulled and deleted from the commercial register (Firmenbuch). The worse could be avoided due to a fast response of the board. However this caused high costs and diverted the team from external projects and acquisition work.

2004 - July: The chief of the finance department had left the company

The time the year-end closing had to be done, all finance employees who were responsible for the books during the past period had left the company, making this task very time consuming and inefficient. This diverted the two finance department staff members from important acquisition work and caused unknown damage by profits foregone.

2004: Plans to convert the uniforce offices for the Austrian Chamber of Industry

These plans would have forced uniforce to find another office. This would have surely become a difficult endeavour, as it is not affiliated to a given university or any other supporting organisation. The main threat would have been that the weekly meetings and office works would have been disrupted, resulting in a more divided team and higher tensions.

2004: Legal threats due to missing trade license (Gewerbeschein)

Since its incorporation, uniforce delivered consulting services to companies

without a company consulting trade license, which is normally required by law. This was due to very stringent requirements a company or individual needed to fulfill before applying for this license. Competing smaller consulting companies supposedly lobbied against uniforce and pushed the Austrian chamber of commerce UBIT to make an example in the industry by bringing uniforce to court. This crisis was solved by registering a senior consultant who fulfilled the requirements as a proxy.

Additionally, alumni responded in interviews that the following problems severely hindered continuous work:

2003-2006: Difficult decision finding at weekly meetings
The time the groups takes to take decisions at weekly meetings exceeds by far the time it spends on external projects, which is certainly unfortunate.

2003: The former management was still member of the group and used its knowledge to block the newly elected management
It was concluded that former management members were to leave the company after their term served.

2001: Low or missing performance by members in the course of external projects
A team member participating in a project team refused to cooperate and do the work agreed upon. This lead to overstraining other team members' resources and to the neglecting of crucial internal and acquisition work. Potential business opportunities were missed and the group motivation sank, resulting in losses difficult to quantify.

C.1.2 Project team

The project team members have the following roles:

Role	Description	Person
Project leader		Michael Schramel
Project manager		Michael Schramel
Risk analyst	prepares and evaluates the risk analyis results	Michael Schramel
Specialist	provides data for the risk analysis	Werner Schmid
Workshop stakeholder	participates to the workshop	Tim Faude, Georg Köldorfer, Hans-Peter Ressel, Sebastian Sieber, Tobias Walkner

C.1.3 Project goals

The goals of this project are the following:

- identify and analyse the past incidents threatening the business continuity of the company
- identify any further risks; quantify their impact and rate of occurrence
- identify safeguards that could lower the costs of risks
- balance the cost of safeguards against the costs of incidents
- develop a strategy and implementation plan to deal with the identified risks using safeguards

C.1.4 Process steps

The steps of this document are depicted in the following figure. It is divided into 3 main phases:

Impact assessment: This phase defines the main risks that could cause an interruption of the essential business processes of the company. It proceeds by defining the essential business processes, the threats and risks, the safeguards and recovery priorities.

Strategy development: This phase develops a strategy to deal with business continuity issues and defines which measures can be implemented and which must be taken.

Implementation and testing plan development: The last phase defines how and when the measures are to be implemented, who is responsible and if/how testing is done.

For the sake of simplicity the last two items are grouped together in C.3.

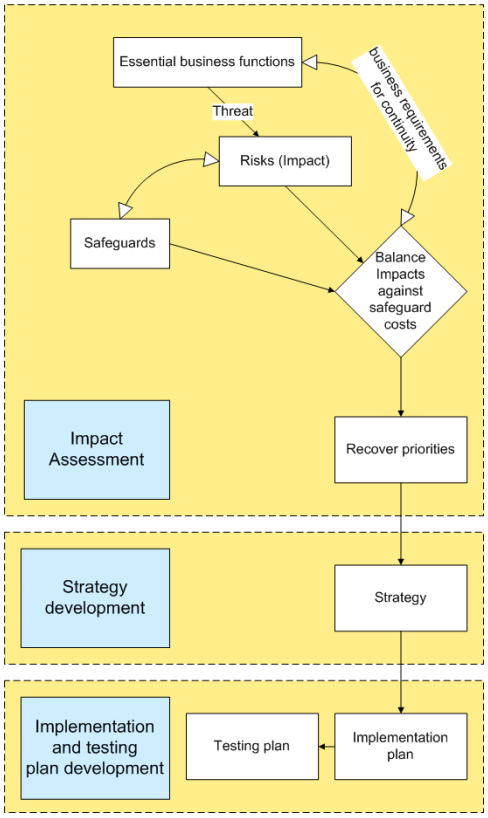


Figure 28: Process steps

This document presents the results of this process.

C.2 Impact assessment and risk analysis

This section presents the main results of the impact assessment phase, including:

- Essential business functions and assets
- Business requirements for continuity and recovery plan parameters
- Threat analysis and risks' impact estimation
- Safeguards and cost-benefit estimation
- Recover priorities

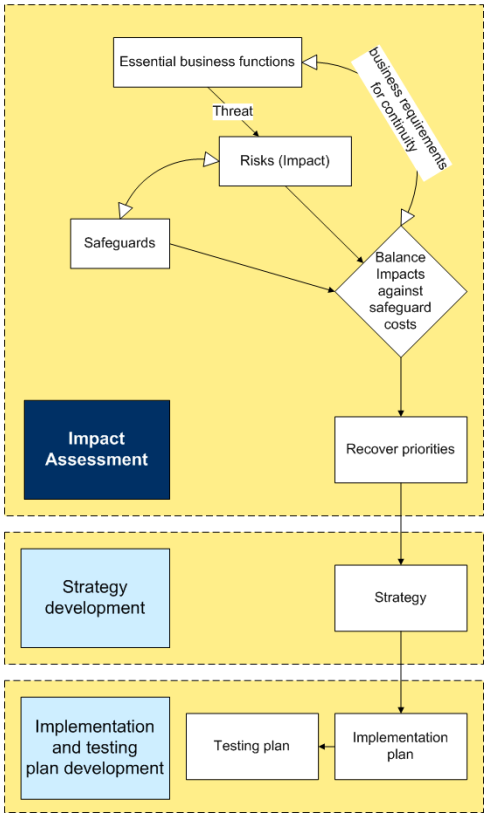


Figure 29: The impact assessment step

C.2.1 Essential business functions

According to a study, 65% of e-business companies which essential business functions are interrupted over a week never reopen and fail. The others lose a large part of their market share. Business continuity management is seen as a mean to avoid the worse case. For this purpose, the main business functions to ensure business continuity need to be identified.

This section presents these main business functions and analyse how they could be disrupted.

Office work: Working at the office requires functioning telecommunication and network systems, PC workstations, fax and kitchen/bathrooms.

Weekly team gathering: The team needs a comfortable, undisturbed private space to gather and discuss the main issues of the daily business to work and communicate efficiently.

Fast customer responses: In order to maintain the company's good image, inquiries of potential and current customers need to be responded quickly. This requires assets

outlined in C.2.1.

Information systems and physical archive: The items relevant for the management of business data are listed in C.2.1.

Legal situation: The incorporation helps the team to present itself professionally and avoids that team members are made liable. It is therefore important that this framework is maintained. Moreover, the physical and virtual infrastructure and processes need to be compliant with relevant regulations.

Financial situation: The company needs to guarantee a certain level of liquidity to cope with unforeseen expenses and risks, and needs to react when this is at stake.

The information security risk analysis identified following critical assets, that could cause a threat to information security if impaired[175]:

- File Server
  - **Project data**
  - **Financial data**
  - Private data
- Web Server
  - Website
  - Extra-net for alumni
  - **Knowledge database for the uniforce team**
  - Internal Blog
  - Budget tool
- Mail Server
  - **uniforce E-Mail services**
  - Jade Austria E-Mail Services
- Groupware server
  - **Customer data**
  - **Team data**
- Backup System (RAID)
  - **RAID device**
  - Backup media (DVDRW)
  - **Backup server**

[175] In **bold** the items selected after positive ratings of the workshop participants.

- Workstations
  - Data stored on workstations
  - 4 Standard systems
  - **1 system with accounting software**
- Home PCs
  - **uniforce data**
  - uniforce email
- Other assets
  - Folders
    - **Accounting folders**
    - **Banking login information**
    - Correspondence folders
    - **Project folders**
  - **Internet connection**
  - the partner's network (chamber of industry)
  - Phone line
  - answering machine
  - fax
  - Video projector

C.2.2 Business requirements for continuity and recovery plan parameters

Following business requirements for the continuity have been identified:

Maintenance of the legal framework: Ensuring that all requirements are met in order to avoid that government agencies threaten the legal existence of the company is crucial for business continuity.

Securing of the company's liquidity: The company needs to be able to deal with unforeseen expenses amounting up.

Securing the security of business critical information: The assets listed in C.2.1 need to held appropriately secured so that incidents can be avoided. This requirement is to be met by the information security workshop in June 2006.

Maintenance of good service levels for internal and external IT services users: Nowadays the inefficient and inappropriate use of IT systems can be highly damaging for the

image of a corporation. This has to be considered when securing the assets listed in C.2.1.

Maintenance of a useful workplace and meeting-room: A place for meetings and office work is essential for the continuity of the company's processes.

Following parameters for a recovery plan are defined:

- Legal problems need to be dealt with highest priority.
- Unforeseen expenses up to 5000 EUR in the lapse of three months must be included in budget planning.
- Company data needs to be secured by all efficient means available and made completely unavailable to non-members.
- Maximal IT systems downtime of 8 hours, i.e. a working day: emails are to be responded within 24h, according to the relevant company policy.
- Each week of the year, a meeting room needs to be available on Wednesdays and a workspace three times a week for three hours each.

C.2.3 Threat analysis and risks' impact estimation

The following business continuity threats were identified as the most dangerous and rated during the risk analysis workshop:

Risk	Likelihood (ARO)	Impact (EUR)
Legal claims due to a failed ext. project	1/5	20.000
Fire	1/100	50.000
Lightning, power outage	1/100	3.000
Loss of corporate sponsorship	1/10	IV:20.000, EI or BM:3.000
unforseen expenses	1/2	3.000
budget abuse	2	4.000

As information security threats play a special role for the business continuity, they were analysed in more detail and presented in the following list:

- Internal (members) and External Threats (hackers, criminals, competitors)
  - Data manipulation
    - **Confidentiality**
    - **Integrity**
    - **Availability (Loss)**

        - (Authentication)
        - non-repudiation
    - **Internet abuse**
    - **Destruction of Hardware**
    - **Vandalism and sabotage**
    - **Social engineering**
    - **Theft of data**
    - **Wiretapping**
- Act of God (fire, flood, lightning, utility break down)
    - **Fire (Loss of data, Process interruption)**
    - Flood (Loss of data, Process interruption)
    - Lightning (Loss of data, Process interruption)
    - **Power break down (Process interruption)**
    - **Internet connection break down (Process interruption)**

C.2.4 Safeguards and cost analysis

During the general business continuity risk analysis, the following safeguards were identified and decided:

Description	Costs	Responsability	Notes
Fire extinguisher	50 EUR	Michael Schramel	maintenance costs?
Fire detector	?	board	if possible
List of assets for insurance claims	-	Georg Köhldorfer	incl. photos
Better project risk analysis	-	QM	by project controller
Better terms and conditions	-	QM	to avoid legal claims
allocation to legal reserves	to be def.	FC	during budget building
turn off computers when not used	-	IT&S	
More care of the sponsor relationships	10-20 h/quarter	CRM+board	
more quality checks in finance	20 h/quarter	QM	
Finance training and test	3 days/year	QM	
Budget rule in partnership agreement	1000 EUR	New bylaws against budget abuse	not selected
New PC adaptors	500 EUR		not selected

In the course of the information security workshop, following safeguards have been discussed[176]:

[176] In **bold** those that have been selected for portfolio computation

- Organisation and infrastructure
  - Cabling
    - Securing of data cables
    - Removal of unused cables
    - Redundant cabling
  - **Employees**
    - **compulsory security training**
    - **security check of new employees**
    - **secure leave of employees**
  - Home office
    - **Home office security concept**
    - Compulsory use of file server when working out-of-office
  - **automatic observation**
  - **Clean workspace**
  - **Identity check by the concierge when providing a key**
  - redundant internet connection
  - **Penetration tests**
  - **secure disposal of old data**
  - **Security Exposure handling plan (project)**
- Physical safegaurds
  - **Key-locked safe for important data**
  - Surveillance camera
- Workstations
  - secure login/password (M4.48)
  - Password protection for accountancy software
  - Creation of a emergency workstation boot disk (CD ROM or DVD) (M 6.78)
  - Compulsory login/log out on workstations for every user
  - **Compulsory use of screen lock**
  - Compulsory use of secure Internet browsers (Mozilla Firefox)
  - Installation of a emergency dual-boot workstation (windows and Linux)
  - workstation backups (M 6.79)
  - Down-grading of Workstation users' role (M2.32)
  - More frequent workstation maintenance

        * Virus scanner installation (M 4.3)
        * Virus software weekly update
        * Operating system updates weekly update
    - Use of BIOS Virus protection
    - Regular BIOS updates
    - Personal firewalls
- Server
    - More frequent backups (M 2.273)
        * daily
        * Every second day
        * **Every fourth day**
    - More frequent server updates
        * automatic
        * every week
        * every 2 weeks
        * every month
    - Server Security Check (NFS, Samba, sendmail, executables) (M 5.82, M 5.17, M 5.18, M 5.19, M 4.23)
    - Creation of a emergency server boot disk (CDROM or DVD) (M 6.24)
    - Monitoring tool for file server
    - Encryption of hard-disk data
    - Database encryption
    - Database rights security check

Implementing the following safeguards at the same time may be yield the following consequences (none of the two was selected):

- Synergies between:
    - Intrusion detection monitor - Monitoring tool for file server
- Exclusion between:
    - Backups daily, every second day, every fourth day

C.2.5 Plan development priorities

For the selection of business continuity measures, two basic criteria were used during the risk analysis workshop: costs and practicability. When in doubt, security measures with high practicability and low costs should be implemented first, as the identified risks are not relevant in the short term and are considered to be under control.

For the selection of the information security safeguard portfolio, the following ALE and cost categories are to be considered with higher priority, as extensive asset data has been collected for this parameters and as they have scored highest in the preparation questionnaires and personal interviews:

- ALE expressed in “Image value for customers (percent)”
- ALE expressed in “Image value for alumni (percent)”
- ALE expressed in “Monetary value (EUR)”
- ALE expressed in “Nonsalaried work (hours)”
- Costs expressed in “Monetary value (EUR)”

The implementation team should bear these parameters in mind and prioritise the implementation of safeguards with favourable ALE reduction values and low costs.

C.3 Strategy and plan development

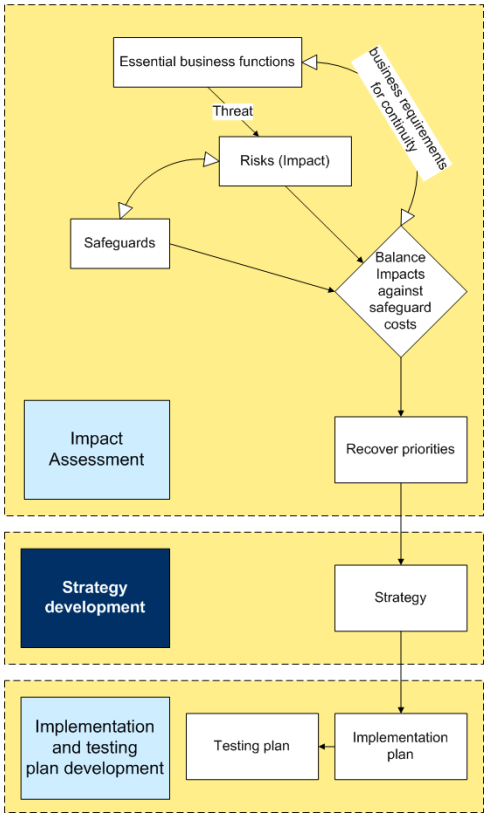


Figure 30: The strategy development step

Management support and team structure The decided safeguards and security measures to assure business continuity and information security are broadly supported by the management and the team, thus helping for their implementation to succeed. The support of two departments has been won:

- The head of IT&S (information technology and services) and CFO participated during the business continuity and information security workshops and has given full commitment to the implementation of the decided measures (Werner Schmid).
- The head of QM (quality management) and FC (finance and controlling) directed the workshop and provided input data (Michael Schramel).

The team implementing the workshop outcomes include one other member working for QM and two other IT&S members (Anna Schwarzbauer, Georg Koehldorfer, Sebastian Sieber).

Strategy selection The selection of the measures to cope with risks, the strategy and the plan to implement them uses the goal set SMART used in the management by objectives

(MBO) method[177]:

S Specific

M Measurable

A Achievable

R Realistic, and

T Time-related

Generally, the chosen strategy should be cost effective and workable. Following business continuity measures have been chosen and will be implemented:

Description	Costs	Responsability	Deadline
New bylaws against budget abuse	1.000 EUR	board	september
Fire extinguisher	50 EUR	Michael Schramel	august
Fire detector	?	board	august
List of assets for insurance claims	-	Georg Köhldorfer	october
Better project risk analysis	-	QM	august
Better terms and conditions (AGB)	-	QM	october
Allocation to legal reserves	to be def.	FC	october
Turn off computers when not used	-	IT&S	july
More care of the sponsor relationships	10-20 h/qr.	CRM+board	september
More quality checks in finance	20 h/qr.	QM	july
Finance training and test	3 days/year	QM	july

Following information security measures have been chosen and will be implemented (in parentheses: the relevant section of the BSI "IT-Sicherheitshandbuch" [Bun05])[178]:

Description	Responsability	Deadline	Sum of costs	Sum of impact reduction
Automatic observation (M4.14)	ITS	October	8	240
Clean workspace	QM	July	24	140
Compulsory security training	ITS	October	36	400
Screen lock	QM	July	45	0
Security exposure handling plan	QM	October	20	480

[177] See http://www.valuebasedmanagement.net/.

[178] NB: the sum of costs and impacts is the sum of user ratings, regardless of the unit employed: it is thus just a coarse and imprecise relative metric for the ranking of the implementation priority of the listed safeguards.

C.4 Summary and outlook

This report presented the results of the preparation, execution and evaluation of a business continuity and information security risk analysis that took place at uniforce junior enterprise GmbH in Vienna, Austria the 7th of June, 2006. Its outcome is to be found in chapter 4 and features eleven decided business continuity measures five information security measures to be implemented until end of October 2006 in joint cooperation between the IT&S and FC&QM departments.

If judged adequate, a second risk analysis workshop will take place in November 2006, which will help to assert the success of the decided and implemented security measures.

D Screenshots of the ReMOSST GDSS brainstorming module

D.1 Cost and value categories

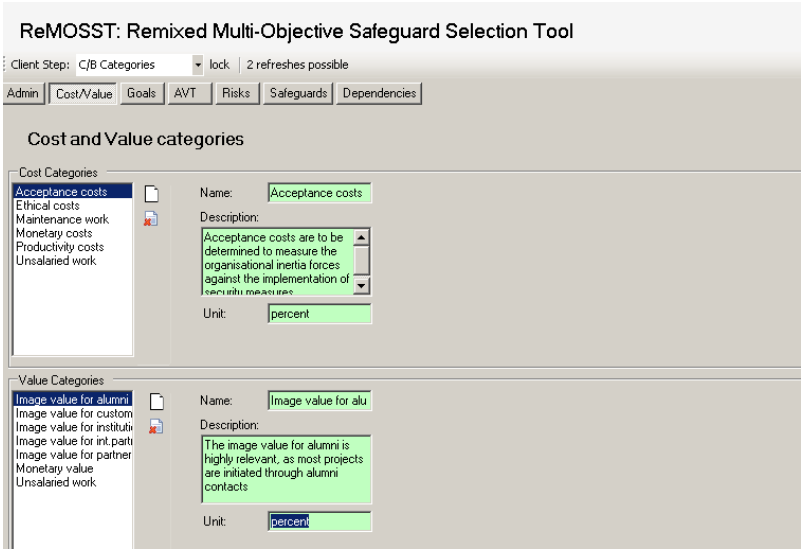


Figure 31: Cost value user interface screenshot

D.2 Goals

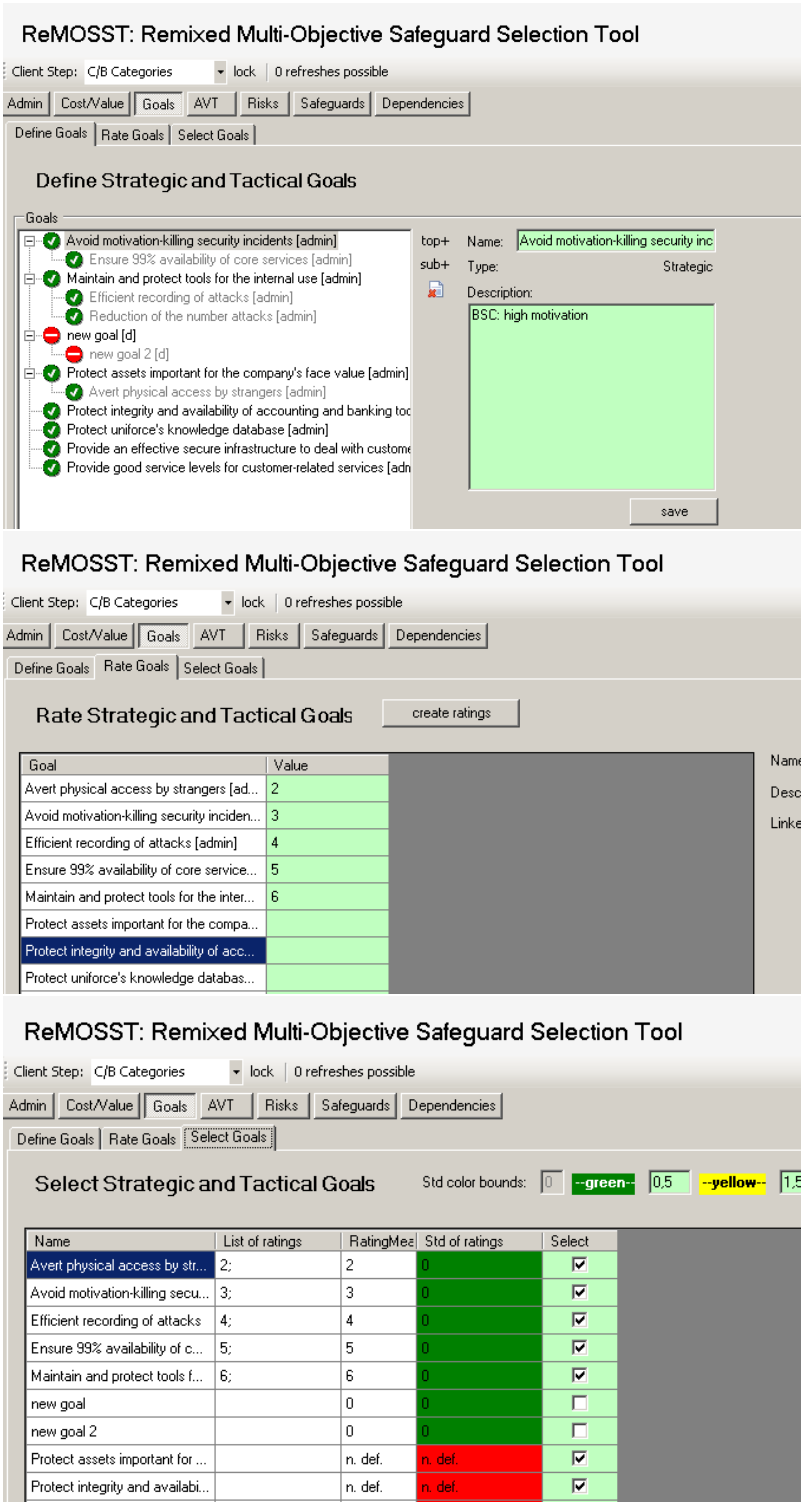


Figure 32: Goal brainstorming, rating and selection user interface screenshots

D.3 Assets, Vulnerabilities and Threats

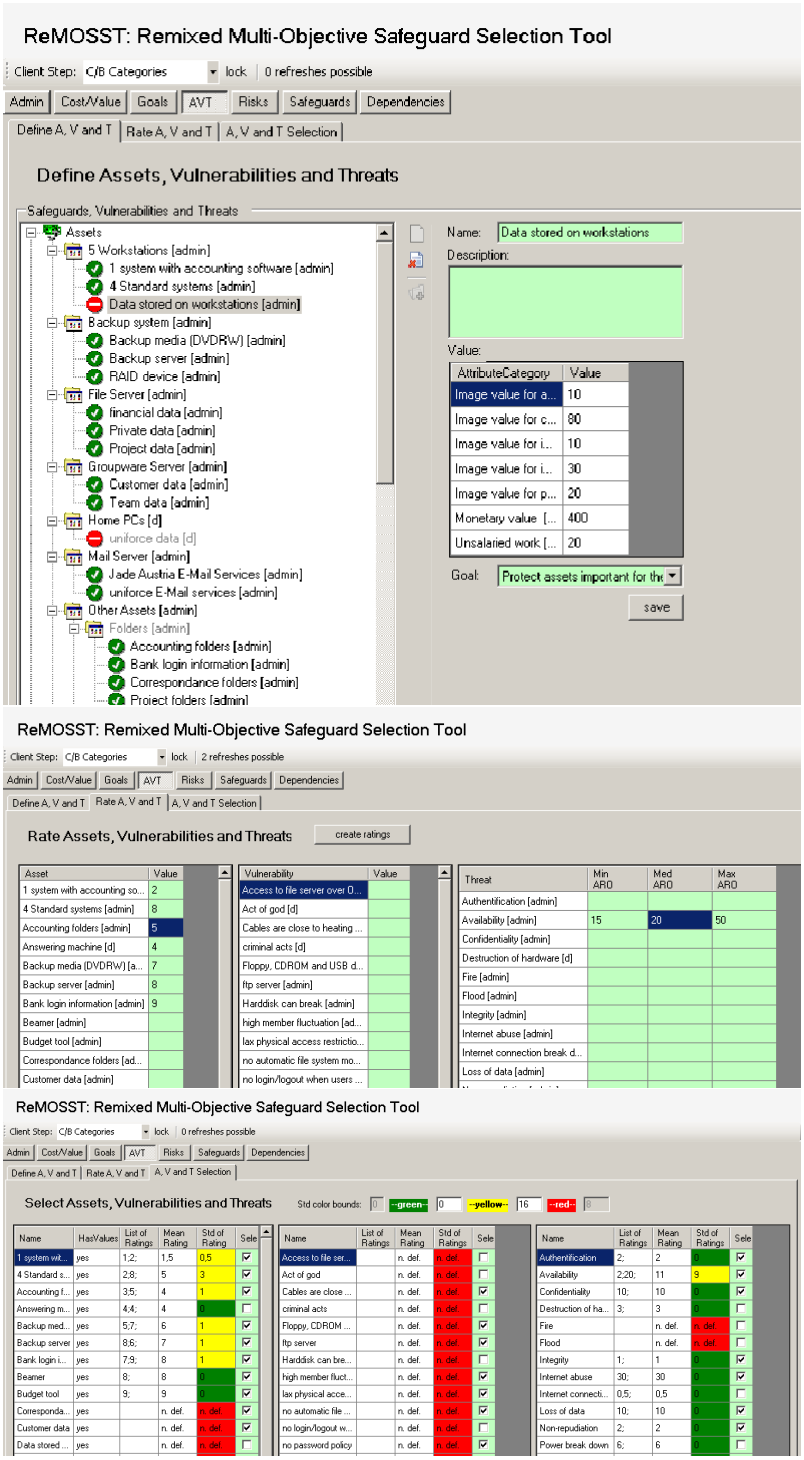


Figure 33: Assets, vulnerabilities and threats brainstorming, rating and selection user interface screenshots

D.4 Risks

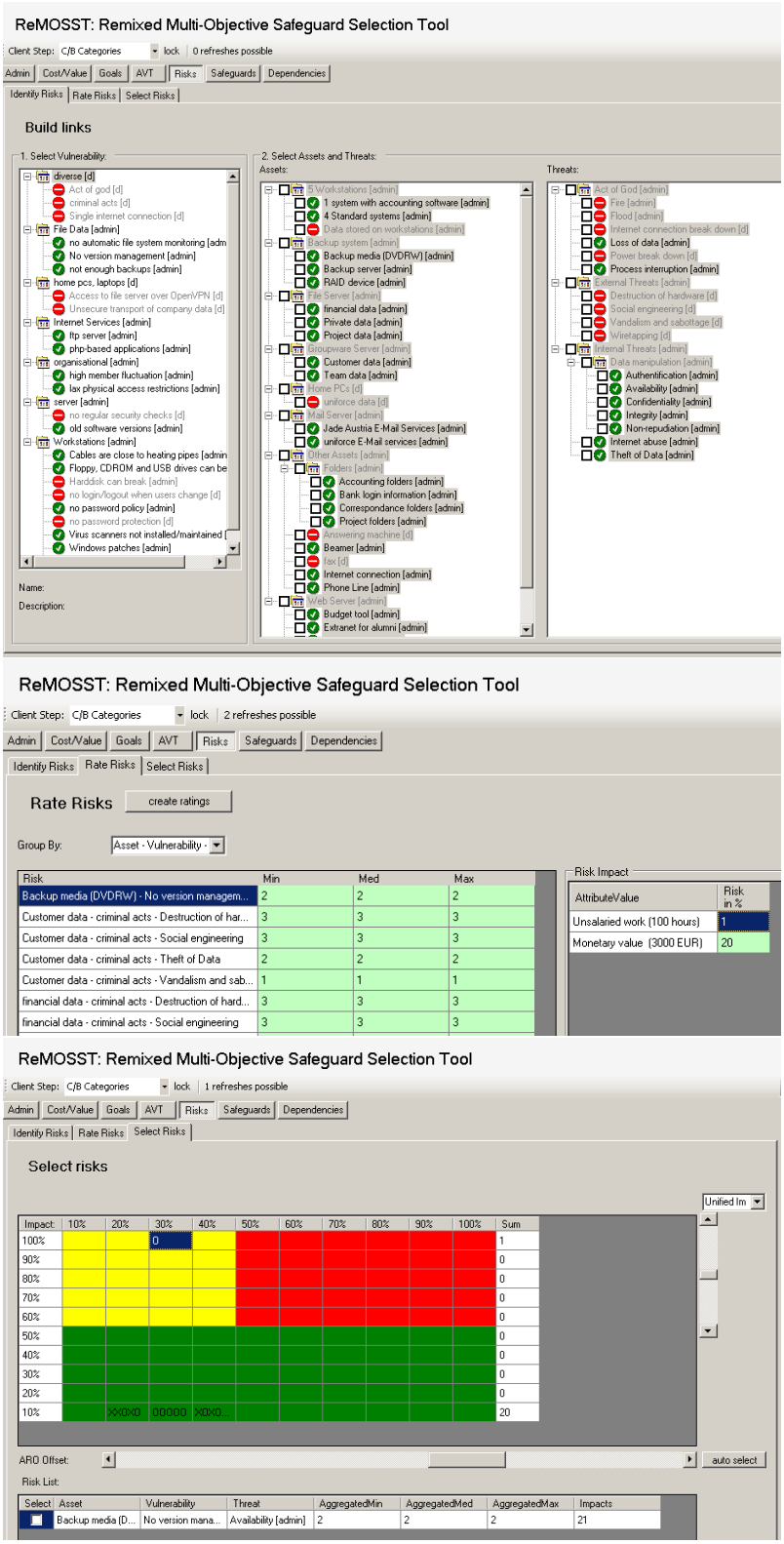


Figure 34: Risk definition, rating and selection user interface screenshots

D.5 Safeguards

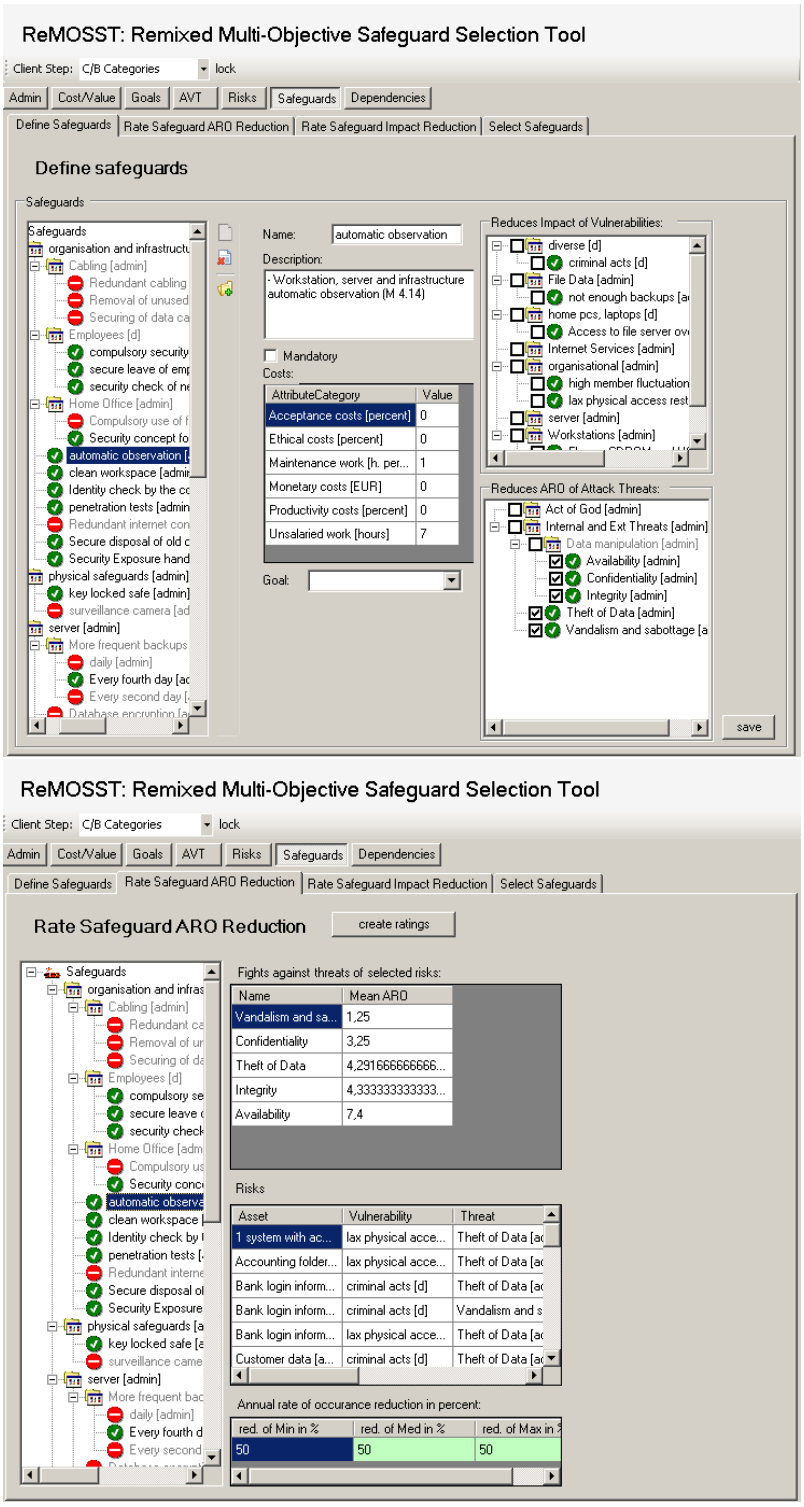


Figure 35: Safeguard definition and rating user interface screenshots

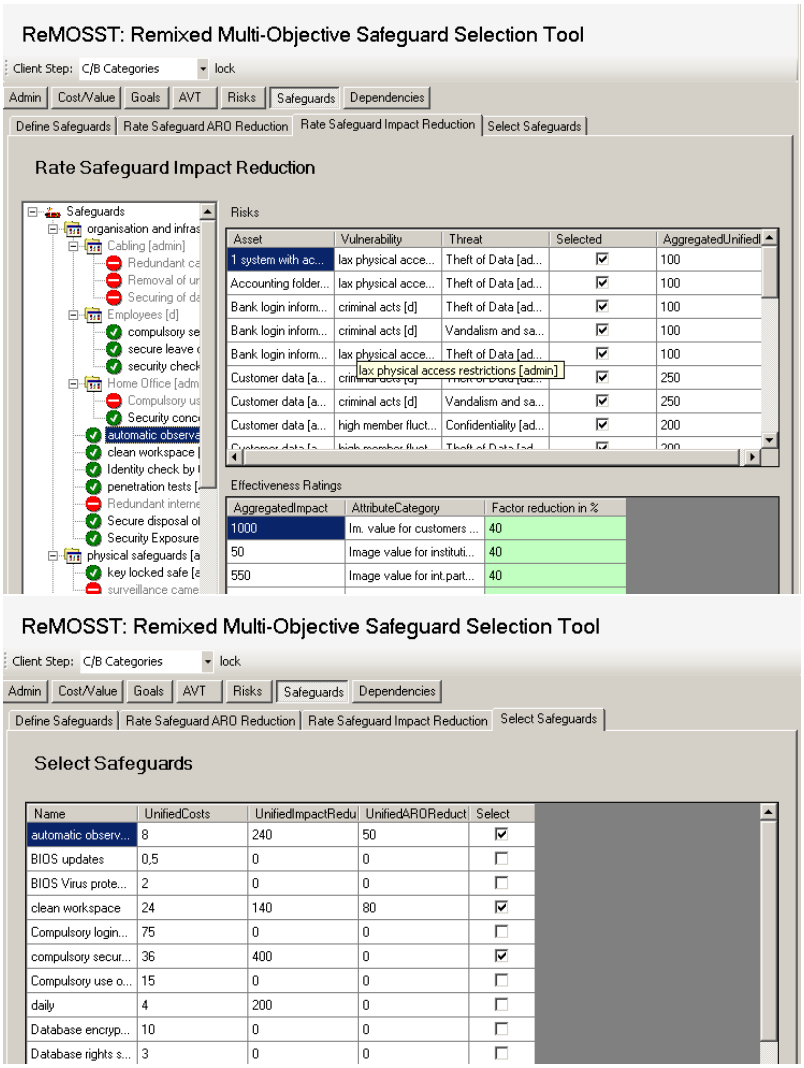


Figure 36: Safeguard rating and selection user interface screenshots

D.6 Dependencies

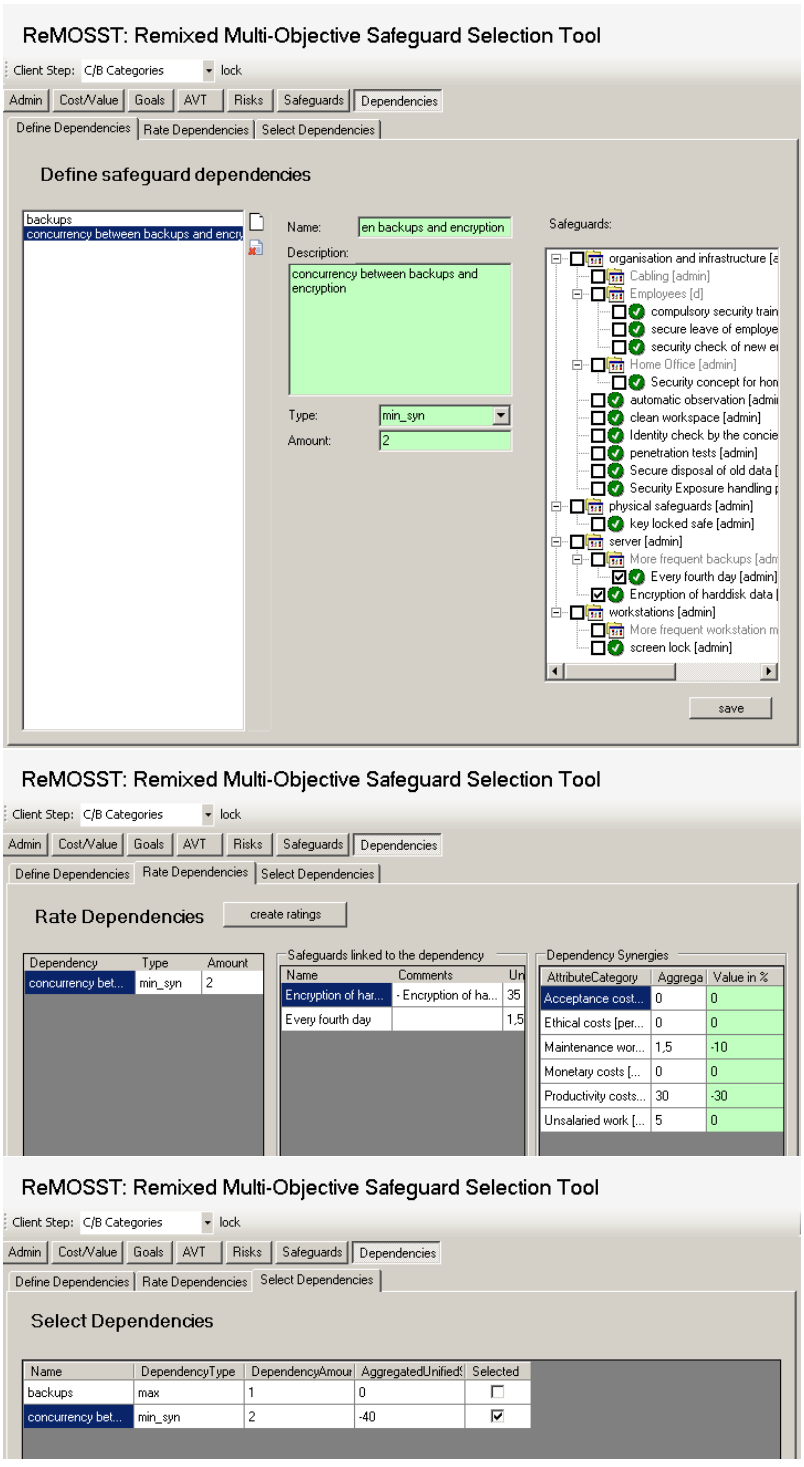


Figure 37: Dependency definition, rating and selection user interface screenshots

E The ReMOSST model applied to a sample portfolio

E.1 Example portfolio data

E.1.1 Assets

The following list of assets are relevant for the computation of the ALE values:

Name	Value in EUR	Value in image (%)	value in recovery time (h)
Webserver	2000	100	25
Mailserver	10.000	80	50
Workstation	1.500	0	8
Laptop	5.000	0	10

E.1.2 Risks

nr.	Asset value	Threat/Vulnerability	min, mode, max ARO	Impact (%)
1	Webserver 100% image	highjacking	0, 1, 5	100
2	Laptop 5.000 EUR	theft of HW/SW	0, 1, 2	100
3	Mailserver 80% image	Denial of service attack	3, 4, 8	40
4	Mailserver 50h	Denial of service attack	2, 5, 8	10

The ARO values are parameters for a triangular distribution. Therefore the mean ARO is calculated by the following formula: $mean = (min + mode + max)/3$.

E.1.3 Portfolio safeguards

nr.	Name	Costs in EUR	Impl. hours	ARO reduction	Impact reduction	Risks
1	open source IDS	0	0	80	60	1,3,4
2	HD encryption	200	5	0	100	2
3	Firewall	1200	30	0	75	4

E.1.4 Portfolio dependencies

Name	Safeguards	Synergies
Net security bundle	IDS+Firewall	-20% in EUR

E.2 Computation of valid portfolios

The following portfolios are valid: [1], [2], [3], [1,2], [1,3], [2,3], [1,2,3]

E.3 Example of the ALE values' computation

Example with two risks and one safeguard: For the following example calculation, the image ALE of portfolio [1,2,3] will be calculated[179]:

Risks that alter the image values: 1 and 3.

$$\begin{aligned} \text{ALE of risk 1} &= 100\,image\,pts * 2\,ARO * 100\%\,impact \\ &= 200\,image\,pts \end{aligned}$$

$$\begin{aligned} \text{ALE of risk 3} &= 80\,image\,pts * 5\,ARO * 40\%\,impact \\ &= 160\,image\,pts \end{aligned}$$

Sum of ALE without safeguards = 360 image pts

Safeguard 1 is the only one that acts on risks 1 and 3.

$$\begin{aligned} \text{ALE of risk 1 with safeguard 1} &= 100\,image\,pts * (2\,ARO * (100\% - 80\%)) \\ &\quad *(100\%\,impact * (100\% - 60\%)) \\ &= 100 * 0.4 * 40\% \\ &= 16\,image\,pts \end{aligned}$$

[179] The ARO value is the mean ARO.

$$\begin{aligned}\text{ALE of risk 3 with safeguard 1} &= 80\,image\,pts * (5\,ARO * (100\% - 80\%)) \\ &\quad *(40\,impact * (100\% - 60\%)) \\ &= 80 * 0.1 * 16\% \\ &= 12.8\,image\,pts\end{aligned}$$

The image ALE value of portfolio [1,2,3] is therefore 28.8.

Example with one risk and two safeguards: For the following example calculation, the recovery time ALE of portfolio [1,2,3] will be calculated:

Risks that alter the recovery time values: 4[180].

$$\begin{aligned}\text{ALE of risk 4} &= 50\,recovery\,time * 5\,ARO * 10\%\,impact \\ &= 25\,recovery\,time\end{aligned}$$

Sum of ALE without safeguards = 25 recovery time

Safeguard 1 and 3 are acting on risks 4.

$$\begin{aligned}\text{ALE of risk 4 with safeg. 1 and 3} &= 50\,recovery\,time * (5\,ARO * (100\% - 80\%) * (100\% - 0\%)) \\ &\quad *(10\%\,impact * (100\% - 60\% * (100\% - 75\%)) \\ &= 50 * 1 * (0.1 * 0.4 * 0.25) \\ &= 0.5\,recovery\,time\end{aligned}$$

The recovery time ALE value of portfolio [1,2,3] is therefore 0.5.

E.4 Example of the cost values' computation

The cost in EUR of the portfolio [1,2,3] is calculated as follows:

[180]The ARO value is the mean ARO.

$$
\begin{aligned}
cost\,in\,EUR &= 0 * (100\% + (-20\%)) + 500 + 1200 * (100\% + (-20\%)) \\
&= 0 + 500 + 960 \\
&= 1460\,EUR
\end{aligned}
$$

Therefore, the cost in EUR of the portfolio [1,2,3] is: 1460 EUR.

E.5 Computation of Pareto optimal portfolios

The ALE values and costs of all valid portfolios are listed in the following table:

	[1]	[2]	[3]	[1,2]	[1,3]	[2,3]	[1,2,3]
Value (EUR)	5000	0	5000	0	5000	0	0
Value in image (%)	28.8	360	360	28.8	28.8	360	28.8
Value in recovery time (h)	25	25	0.5	25	0.5	0.5	0.5
Costs (EUR)	0	500	1200	500	960	1700	1460
Implementation time (EUR)	0	5	30	5	30	35	35

This list is reduced by the portfolios that can be proven to be dominated by another one[181].

In this case, [1,2,3] dominates [2,3], [1,2] dominates [2] and [1,3] dominates [3]. Accordingly, the Pareto optimal portfolios are the following: [1], [1,2], [1,3] and [1,2,3].

E.6 Monte Carlo simulation

ReMOSST simulates a ALE distribution using a Monte Carlo simulation, described in 8.3.3. The following example presents a simulation of the image ALE value of portfolio [1,2,3]:

$$
\begin{aligned}
\text{ALE of risk 1 with safeguard 1} &= 100\,image\,pts * (x_1\,ARO * (100\% - 80\%)) \\
&\quad *(100\%\,impact * (100\% - 60\%)) \\
&\quad +80\,image\,pts * (x_3\,ARO * (100\% - 80\%)) \\
&\quad *(40\%\,impact * (100\% - 60\%)) \\
x_1 &\quad randomly\,generated\,ARO\,of\,risk\,1 \\
x_3 &\quad randomly\,generated\,ARO\,of\,risk\,3
\end{aligned}
$$

[181] A portfolio dominates another one if all his ALE values and costs are lower or equal.

Given two random number $r_1$and r_3 uniformly distributed between 0 and 1, $x_1$and $x_3$can be calculated using the following formula, described in 8.3.3, where $i \in \{1, 3\}$:

$$\begin{cases} x_i = \sqrt{r_i(max_i - min_i)(mode_i - min_i)} + min_i & if\ 0 \leq r_i \leq \frac{mode_i - min_i}{max_i - min_i} \\ x_i = max_i - \sqrt{(1 - r_i)(max_i - min_i)(max_i - mode_i)} & if\ \frac{mode_i - min_i}{max_i - min_i} < r_i \leq 1 \end{cases}$$

A Monte Carlo simulation with 7 iterations would generate the following output:

r_1	r_3	x_1	x_3	ALE_1	ALE_3	ALE sum
0.3	0.7	1.258	5.551	10.07	14.21	24.28
0.1	0.2	0.707	4.000	5.66	10.24	15.90
0.8	0.6	3.000	5.172	24.00	13.24	37.24
0.8	0.8	3.000	6.000	24.00	15.36	39.36
0.9	0.6	3.586	5.172	28.69	13.24	41.93
0.7	0.6	2.551	5.172	20.40	13.24	33.64
0.9	0.95	3.586	7.000	28.69	17.92	46.61

The mean value of the portfolios image ALE sample is 34.14, its standard deviation is 10.67.

F The data collected during the uniforce workshop

F.1 Cost and value categories

Name	Unit	AttributeType
Im. value for customers	percent	Asset value
Image value for partners	percent	Asset value
Monetary costs	EUR	Sfg. cost
Image value for institutional supporters	percent	Asset value
Img. value for alumni	percent	Asset value
Monetary value	EUR	Asset value
Acceptance costs	percent	Sfg. cost
Ethical costs	percent	Sfg. cost
Maintenance work	h. per week	Sfg. cost
Unsalaried work	hours	Sfg. cost
Image value for int.partners	percent	Asset value
Productivity costs	percent	Sfg. cost
Unsalaried work	hours	Asset value

F.2 Goals

Name	Selected
Avert physical access by strangers	True
Protect uniforce s knowledge database	True
Efficient recording of attacks	True
Avoid motivation-killing security incidents	True
Provide an effective secure infrastructure to deal with customer inquiries	True
Provide good service levels for customer-related services	True
Protect assets important for the company’s face value	True
Reduction of the number attacks	True
Ensure 99 percent availability of core services	True
Maintain and protect tools for the internal use	True
Protect integrity and availability of accounting and banking tools	True

F.3 Assets

Name	Selected	RatingsList	R.Mean	R.Std
Customer data	True	4;3;5;5;	4,25	0,829
Internet connection	True	5;3;2;3;	3,25	1,09
Video projector	False	1;3;1;1;	1,5	0,866
Internal Blog	False	3;1;1;2;	1,75	0,829
4 Standard systems	False	1;1;2;2;	1,5	0,5
fax	False	1;1;1;1;	1	0
Accounting folders	True	5;3;5;2;	3,75	1,299
1 system with accounting SW	True	4;2;4;5;	3,75	1,09
Jade Austria E-Mail Services	False	1;1;3;5;	2,5	1,658
Correspondance folders	False	2;5;1;2;	2,5	1,5
Data stored on workstations	False	1;5;1;1;	2	1,732
Knowledge database	True	5;5;3;5;	4,5	0,866
Private data	False	1;1;5;2;	2,25	1,639
Phone Line	False	3;1;1;1;	1,5	0,866
Backup server	True	5;5;5;5;	5	0
uniforce E-Mail services	True	4;4;5;5;	4,5	0,5
Project data	True	2;5;4;5;	4	1,225
Extranet for alumni	False	4;2;1;2;	2,25	1,09
uniforce email	False		0	0
Project folders	True	5;2;5;5;	4,25	1,299
Web Site	False	1;	1	0
Bank login information	True	5;4;3;4;	4	0,707
Budget tool	False	1;4;1;2;	2	1,225
financial data	True	5;4;5;5;	4,75	0,433
Team data	True	4;4;1;4;	3,25	1,299
Answering machine	False	1;2;1;1;	1,25	0,433
uniforce data	True	3;3;5;4;	3,75	0,829
RAID device	True	5;4;2;5;	4	1,225

Asset Values of Customer data

Category	Value
Monetary value [EUR]	2000
Unsalaried work [hours]	100
Im. value for customers [percent]	100

Asset Values of Internet connection

Category	Value
Monetary value [EUR]	2000
Image value for institutional supporters [percent]	100

Asset Values of Video projector

Category	Value
Image value for institutional supporters [percent]	100
Monetary value [EUR]	2500

Asset Values of Internal Blog

Category	Value
Unsalaried work [hours]	20

Asset Values of 4 Standard systems

Category	Value
Unsalaried work [hours]	20

Asset Values of fax

Category	Value
Image value for int.partners [percent]	30
Im. value for customers [percent]	100
Monetary value [EUR]	600
Image value for partners [percent]	100
Image value for institutional supporters [percent]	30
Img. value for alumni [percent]	30
Unsalaried work [hours]	5

Asset Values of Accounting folders

Category	Value
Unsalaried work [hours]	100

Asset Values of 1 system with accounting software

Category	Value
Unsalaried work [hours]	5
Monetary value [EUR]	200

Asset Values of Jade Austria E-Mail Services

Category	Value
Unsalaried work [hours]	10

Asset Values of Correspondance folders

Category	Value
Unsalaried work [hours]	250
Monetary value [EUR]	1000

Asset Values of Data stored on workstations

Category	Value
Image value for institutional supporters [percent]	10
Unsalaried work [hours]	20
Img. value for alumni [percent]	10
Monetary value [EUR]	400
Image value for partners [percent]	20
Image value for int.partners [percent]	30
Im. value for customers [percent]	80

Asset Values of Knowledge database

Category	Value
Monetary value [EUR]	500
Unsalaried work [hours]	200

Asset Values of Private data

Category	Value
Unsalaried work [hours]	50
Img. value for alumni [percent]	80

Asset Values of Phone Line

Category	Value
Image value for institutional supporters [percent]	100
Monetary value [EUR]	1000
Image value for int.partners [percent]	100
Im. value for customers [percent]	100
Image value for partners [percent]	100
Img. value for alumni [percent]	100

Asset Values of Backup server

Category	Value
Unsalaried work [hours]	25
Monetary value [EUR]	500

Asset Values of uniforce E-Mail services

Category	Value
Unsalaried work [hours]	50

Asset Values of Project data

Category	Value
Monetary value [EUR]	10000
Unsalaried work [hours]	1000
Image value for int.partners [percent]	100
Img. value for alumni [percent]	70
Im. value for customers [percent]	100

Asset Values of Extranet for alumni

Category	Value
Img. value for alumni [percent]	100
Unsalaried work [hours]	150

Asset Values of uniforce email

Category	Value
Im. value for customers [percent]	10
Monetary value [EUR]	100

Asset Values of Project folders

Category	Value
Unsalaried work [hours]	250

Asset Values of Web Site

Category	Value
Unsalaried work [hours]	200
Im. value for customers [percent]	100
Image value for partners [percent]	100
Monetary value [EUR]	3500
Image value for institutional supporters [percent]	100
Image value for int.partners [percent]	100
Img. value for alumni [percent]	100

Asset Values of Bank login information

Category	Value
Monetary value [EUR]	10000

Asset Values of Budget tool

Category	Value
Monetary value [EUR]	500
Unsalaried work [hours]	50

Asset Values of financial data

Category	Value
Monetary value [EUR]	5000
Unsalaried work [hours]	200

Asset Values of Team data

Category	Value
Unsalaried work [hours]	100

Asset Values of Answering machine

Category	Value
Img. value for alumni [percent]	30
Image value for int.partners [percent]	20
Monetary value [EUR]	100
Im. value for customers [percent]	100
Image value for partners [percent]	100
Image value for institutional supporters [percent]	100

Asset Values of uniforce data

Category	Value
Unsalaried work [hours]	100
Monetary value [EUR]	1000

Asset Values of RAID device

Category	Value
Monetary value [EUR]	300
Image value for institutional supporters [percent]	50

F.4 Threats

Name	Selected	RatingsList	RatingMean	RatingStd
Confidentiality	True	2;1;5;5;	3,25	1,785
Vandalism and sabottage	True	1;1;	1,25	0,25
Internet abuse	True	6;3;20;12;	10,25	6,495
Integrity	True	3;3;5;5;	4,33	1,053
Social engineering	True	1;1;1;	1	0
Theft of Data	True	1;10;3;3;	4,29	3,419
Lightning	False	0,01;0,001;0,05;0;	0,02	0,021
Internet connection break down	True	1;8;4;1,5;	3,96	2,79
Destruction of hardware	True	1;3;5;4;	3,5	1,5
Authentification	False	30;3;6;5;	12,67	11,148
Flood	False	0;0,01;0,05;0,001;	0,02	0,021
Availability	True	1;3;3;3;20;	7,4	7,181
Fire	True	0;0,01;0,05;0,01;	0,02	0,019
Power break down	True	5;0,01;0,1;1;	1,53	2,042
Non-repudiation	False	6;6;3;	5,22	1,431

F.5 Vulnerabilities

Name	Selected	RatingsList	R.Mean	R.Std
criminal acts	True	1;2;2;4;	2,25	1,09
Single internet connection	False	1;2;2;	1,67	0,471
No version management	True	3;1;3;3;	2,5	0,866
no password protection	True	2;4;4;5;	3,75	1,09
Unsecure transport of company data	False	2;1;1;3;	1,75	0,829
Workstations are not turned off	False		0	n. def.
Harddisk can break	True	4;4;5;5;	4,5	0,5
no regular security checks	True	2;3;2;3;	2,5	0,5
high member fluctuation	True	3;4;4;5;	4	0,707
Access to file server over OpenVPN	True	4;3;5;5;	4,25	0,829
Windows patches	True	2;4;2;4;	3	1
no password policy	True	3;2;4;3;	3	0,707
Cables are close to heating pipes	False	2;1;1;2;	1,5	0,5
Floppy, CDROM and USB drives can be used	True	2;2;3;4;	2,75	0,829
no login/logout when users change	True	2;4;2;2;	2,5	0,866
no automatic file system monitoring	False	3;2;1;1;	1,75	0,829
lax physical access restrictions	True	3;3;5;4;	3,75	0,829

not enough backups	True	4;5;5;3;	4,25	0,829
Act of god	False	1;1;2;1;	1,25	0,433
old software versions	False	1;2;2;1;	1,5	0,5
ftp server	False	5;5;1;2;	3,25	1,785
Virus scanners not installed/maintained	True	2;1;4;4;	2,75	1,299
php-based applications	False	2;1;2;1;	1,5	0,5

F.6 Safeguards

Name	Selected
Virus scanner installation	False
Securing of data cables	False
daily	False
compulsory security training	True
workstation backups	False
screen lock	True
penetration tests	True
BIOS Virus protection	False
Security concept for home work	True
Database rights security check	False
Password protection for accountancy software	False
surveillance camera	False
Compulsory login/logout	False
Database encryption	False
file server monitoring	False
Personal firewalls	False
Lesser user role	False
security check of new employees	True
Every second day	False
emergency workstation boot disk	False
Encryption of harddisk data	True
Secure disposal of old data	True
Removal of unused cables	False
Identity check by the concierge when providing a key	True
Redundant cabling	False
secure leave of employees	True
secure internet browsers	False
Compulsory use of file server when working out-of-office	False
OS updates weekly	False

clean workspace	True
PGP-signed/-encrypted mails	False
Redundant internet connection	False
emergency server boot disk	False
automatic observation	True
BIOS updates	False
dual-boot workstation	False
Virus scan for incoming emails	False
IDS	False
Security Exposure handling plan	True
secure login/password	False
Virus software weekly update	False
key locked safe	True
Every fourth day	True
Server Security Check	False

Safeguard Costs of Virus scanner installation

Category	Value
Productivity costs [percent]	1
Maintenance work [h. per week]	0,5
Unsalaried work [hours]	2

Safeguard Costs of Securing of data cables

Category	Value
Unsalaried work [hours]	8
Monetary costs [EUR]	50

Safeguard Costs of daily

Category	Value
Maintenance work [h. per week]	4

Safeguard Costs of compulsory security training

Category	Value
Maintenance work [h. per week]	1
Productivity costs [percent]	-5
Acceptance costs [percent]	30
Unsalaried work [hours]	10

Safeguard Costs of workstation backups

Category	Value
Maintenance work [h. per week]	2
Unsalaried work [hours]	10

Safeguard Costs of screen lock

Category	Value
Productivity costs [percent]	5
Acceptance costs [percent]	40

Safeguard Costs of penetration tests

Category	Value
Unsalaried work [hours]	15

Safeguard Costs of BIOS Virus protection

Category	Value
Unsalaried work [hours]	2

Safeguard Costs of Security concept for home work

Category	Value
Unsalaried work [hours]	20
Maintenance work [h. per week]	2

Safeguard Costs of Database rights security check

Category	Value
Unsalaried work [hours]	3

Safeguard Costs of Password protection for accountancy software

Category	Value
Unsalaried work [hours]	2
Acceptance costs [percent]	10

Safeguard Costs of surveillance camera

Category	Value
Acceptance costs [percent]	40
Monetary costs [EUR]	250
Maintenance work [h. per week]	2
Unsalaried work [hours]	5
Ethical costs [percent]	80

Safeguard Costs of Compulsory login/logout

Category	Value
Productivity costs [percent]	30
Acceptance costs [percent]	40
Maintenance work [h. per week]	1
Unsalaried work [hours]	4

Safeguard Costs of Database encryption

Category	Value
Unsalaried work [hours]	5
Productivity costs [percent]	5

Safeguard Costs of file server monitoring

Category	Value
Maintenance work [h. per week]	0,5
Unsalaried work [hours]	3

Safeguard Costs of Personal firewalls

Category	Value
Maintenance work [h. per week]	0,2
Unsalaried work [hours]	3

Safeguard Costs of Lesser user role

Category	Value
Acceptance costs [percent]	30
Unsalaried work [hours]	10
Productivity costs [percent]	40
Maintenance work [h. per week]	2

Safeguard Costs of security check of new employees

Category	Value
Maintenance work [h. per week]	2
Acceptance costs [percent]	1

Safeguard Costs of Every second day

Category	Value
Maintenance work [h. per week]	2,5

Safeguard Costs of emergency workstation boot disk

Category	Value
Unsalaried work [hours]	4

Safeguard Costs of Encryption of harddisk data

Category	Value
Productivity costs [percent]	30
Unsalaried work [hours]	5

Safeguard Costs of Secure disposal of old data

Category	Value
Maintenance work [h. per week]	0,5

Safeguard Costs of Removal of unused cables

Category	Value
Unsalaried work [hours]	5

Safeguard Costs of Identity check by the concierge when providing a key

Category	Value
Unsalaried work [hours]	3
Maintenance work [h. per week]	1
Acceptance costs [percent]	60

Safeguard Costs of Redundant cabling

Category	Value
Unsalaried work [hours]	5
Monetary costs [EUR]	50

Safeguard Costs of secure leave of employees

Category	Value
Maintenance work [h. per week]	2

Safeguard Costs of secure internet browsers

Category	Value
Unsalaried work [hours]	2
Acceptance costs [percent]	10

Safeguard Costs of Compulsory use of file server when working out-of-office

Category	Value
Acceptance costs [percent]	20
Productivity costs [percent]	-5

Safeguard Costs of OS updates weekly

Category	Value
Unsalaried work [hours]	1

Safeguard Costs of clean workspace

Category	Value
Productivity costs [percent]	-20
Maintenance work [h. per week]	4
Acceptance costs [percent]	40

Safeguard Costs of PGP-signed/-encrypted mails

Category	Value
Maintenance work [h. per week]	0,5
Acceptance costs [percent]	50
Productivity costs [percent]	10
Unsalaried work [hours]	5

Safeguard Costs of Redundant internet connection

Category	Value
Maintenance work [h. per week]	0,5
Monetary costs [EUR]	200
Unsalaried work [hours]	25

Safeguard Costs of emergency server boot disk

Category	Value
Unsalaried work [hours]	5
Maintenance work [h. per week]	0,5

Safeguard Costs of automatic observation

Category	Value
Unsalaried work [hours]	7
Maintenance work [h. per week]	1

Safeguard Costs of BIOS updates

Category	Value
Maintenance work [h. per week]	0,5

Safeguard Costs of dual-boot workstation

Category	Value
Unsalaried work [hours]	5

Safeguard Costs of Virus scan for incoming emails

Category	Value
Acceptance costs [percent]	10
Productivity costs [percent]	15
Ethical costs [percent]	15
Unsalaried work [hours]	8
Maintenance work [h. per week]	0,5

Safeguard Costs of IDS

Category	Value
Unsalaried work [hours]	5
Maintenance work [h. per week]	1

Safeguard Costs of Security Exposure handling plan

Category	Value
Unsalaried work [hours]	20

Safeguard Costs of secure login/password

Category	Value
Acceptance costs [percent]	40
Unsalaried work [hours]	3

Safeguard Costs of Virus software weekly update

Category	Value
Maintenance work [h. per week]	1

Safeguard Costs of key locked safe

Category	Value
Monetary costs [EUR]	300

Safeguard Costs of Every fourth day

Category	Value
Maintenance work [h. per week]	1,5

Safeguard Costs of Server Security Check

Category	Value
Unsalaried work [hours]	10
Maintenance work [h. per week]	1,5

F.7 Dependencies

Name
backups
concurrency between backups and encryption

Safeguards included in dependency backups

Name
daily
Every fourth day
Every second day

Synergies of dependency backups

User	Cost category	Value in percent pts

Safeguards included in dependency concurrency between backups and encryption

Name
Encryption of harddisk data
Every fourth day

Synergies of dependency concurrency between backups and encryption

User	Cost category	Value in percent pts
admin	Maintenance work [h. per week]	-10
admin	Unsalaried work [hours]	0
admin	Acceptance costs [percent]	0
admin	Productivity costs [percent]	-30
admin	Ethical costs [percent]	0
admin	Monetary costs [EUR]	0