MASTER THESIS

QUANTIFIED RETURN ON INFORMATION SECURITY INVESTMENT
- A MODEL FOR COST-BENEFIT ANALYSIS

Panchit Puangsri

MASTER THESIS

QUANTIFIED RETURN ON INFORMATION SECURITY INVESTMENT

- A Model for Cost-Benefit Analysis

Ms. Panchit Puangsri, 1381555, MSc. in Management of Technology
Department of Technology, Policy and Management
Delft University of Technology

Chairman: Marijn Janssen (Information and Communication Technology)
First supervisor: Jan van den Berg (Information and Communication Technology)
Second supervisor: John Groenewegen (Economics of Infrastructures)
TNO supervisor: Femke Hulsbergen-Sletering


TU Delft

EXECUTIVE SUMMARY

In this thesis, the research question is "*in which way can the relation between IT-security incidents and their impacts be modelled to conduct the quantitative cost-benefit analysis for information security investment?*" The motivation for this research has been that there is a need for a better quantitative model for an information security investment to compete for a budget with other business opportunities. Derived from the model, an application is built to provide results of quantified return on information security investment (ROISI). Several approaches are explored to support expert estimate and to deal with uncertainty existing in the information security world.

During the research, a security risk management approach is explored. The *five* phases presented are risk analysis, risk assessment, strategy selection, cost-benefit analysis and implementation. First, assets, threats and vulnerabilities of the IT systems are identified in the *risk analysis* phase. This assists in identifying possible IT-security incidents. Second, to assess each incident, their impact and likelihood are quantitatively assessed in the *risk assessment* phase. Additionally, uncertainty in estimates from the impact and the likelihood is possibly assessed in this phase as well. Third, one of the strategies (acceptance, avoidance, transference and mitigation) is selected to handle risks in the *strategy selection* phase. Fourth, an information security investment is assessed in the *cost-benefit analysis* phase. Fifth, the *implementation* phase is conducted when results from ROISI are favourable. Since the security risk management process is a continuing process, the evaluation part for residual risks gives a loopback to the first phase.

Next, Return on Information Security Investment or ROISI is an approach assessing an information security investment employing the cost-benefit analysis. To quantitatively assess the investment, first the *benefit of controls* can be computed from loss reduced due to the security investment. There are *two* approaches quantifying risks. When risks can be acceptably defined as a product of the *likelihood* and the *impact*, many experts agree to apply the Annual Loss Expectancy or the ALE methodology representing the annually expected financial loss. The *first* approach measures security risk from the ALE derived from direct estimates of the impact and the likelihood. From the *impact* assessment, the Single Loss Exposure or the SLE indicates loss resulted from a single occurrence of a risk. The impact of an IT-security incident can be derived from lost revenue, regulatory penalty, lost productivity and reputation loss. Due to the project scope, lost productivity and reputation loss are excluded. For lost revenue and regulatory penalty, the important quantifiable elements are loss of sale, damage to asset, cost of recovery for software, hardware, internal employee and external consultant, and regulatory penalty. From the *likelihood* assessment, the Annual Rate of Occurrence or the ARO indicates the frequency that the risk may occur in one year. The *second* approach conducting the quantitative risk assessment applies from the qualitative technique. The impact and/or likelihood level of a risk can be classified into several levels such as low, medium and high and then these levels are assigned a numeric value for their expected loss and/or frequency. From here the SLE, the ARO and therefore

the ALE are numerically identified. Next, the *cost of controls* is divided into *two* parts. *First*, the set-up cost is expenditure paid to design, establish and start using an information security system, while, *second*, the recurring cost is annual expenditure recurred to maintain the system operating. The set-up cost generally consists of software, license fee, hardware, consultancy on analysis and configuration, training and facility, whereas the recurring cost often consists of support and maintenance fee and human resource for monitoring.

With the numeric results of costs and benefits, there exist *three* well-known approaches to execute ROISI namely the ROI/ROISI, the NPV and the IRR. In this research, another approach called the discount ROISI or the dROISI is developed by combining the NPV and the ROISI. To conclude, the ROI/ROISI is the most popular and the least complex method since it does not take time value of money into account. So this method does not discount cash flows to their present value. However, all methods using time value of money face a problem of limited information. The NPV is the only approach informing about the magnitude of the project. Lastly, the IRR has a doubtful assumption because it assumes that the whole period of time has the same rate of return. Each approach is better match to different cases. More detail can be found in the last chapter. Overall, a decision maker should use a combination of methods to justify investment opportunities in general.

Combining the benefits and the costs, the relation between IT-security incidents and their impacts can be modelled to conduct the quantitative cost-benefit analysis for information security investment in the way illustrated later in the report. Starting from a company possessing valuable information assets, some information assets are at stake. These assets are endangered by IT-security threats and if the threats are materialized to be incidents, this will cause losses. Then as a part of IT budget, IT security budget can be used for establishing and maintaining an information security system with the costs explained earlier. The viability of an investment can be tested with the benefits from reduced losses against the costs. According to the models developed, an ROISI application is developed, shown in chapter 5. According to expert interviews, the models seem to be rather practical, good, clear and useful and the application receives very positive feedbacks, especially when applied to a detailed risk assessment analysis. However the application may need an adjustment when being applied to some specific cases in order to better fit in different situations.

Lastly, several approaches are needed to support expert estimation and to deal with uncertainty. *First* of all, *disaggregation*, which splits an estimate into smaller elements, can be applied to help experts to give better estimates for the impact. *Second* it is recommended to give an expert *feedback* and *training* and to combine more than one expert's opinions (*multiple-expert estimate*) to reduce bias and increase reliability. *Third*, the *Monte Carlo approach* may be applied with the likelihood estimation to provide more realistic information about the results to decision makers; however, it is still doubtful whether it is practically beneficial for a company. Because it requires additional information about the probability distribution, which could be very time consuming. To sum up, in a case that complexity is low and experts have knowledge of probability distribution, it is worthwhile to apply the Monte Carlo approach. On the other hand, in a case that complexity is high and experts' degree of belief is low, we do not recommend a company to apply the Monte Carlo approach to ROISI. *Fourth* and finally, *sensitivity analysis* can be applied to give better understanding of the model structure and the main sources or inputs of model output uncertainty.

These are the main important results of this thesis fulfilling the problem statement. Please note here that the models and the application are a first attempt in making a true quantitative model but in order to make the models and the application more accurate and more useful in practice, it still needs further researches.

FOREWORD

To fulfil the requirements for the degree of MSc in Management of Technology at Delft University of Technology, this master thesis was conducted in the six-month period between the mid of February and August 2009. It is in a combination with an internship at the Strategy Business Analysis unit in the Innovation Management department in TNO ICT, while collaborating with Security unit in the Information Technology department. After the whole period of very hard work, I have some words of thanks to many important persons who have a part of this thesis success.

First of all, I would like to thank Jan van den Berg, my first supervisor, and Femke Hulsbergen, my TNO supervisor. Thanks to their endless patience reading my thesis over and over again and to their invaluable advices and discussions to help me best improve my research. Because of both of them, I could make it possible to graduate in time as one of a few, even though I got started one month and a half later than most other students. Besides this, those informal conversations we had did comfort me through the whole period of very hard work.

Next I want to thank people from the Strategic Business Analysis unit in TNO ICT for comforting me while working at TNO, especially many thanks to Frank Berkers for introducing me to this topic, Thomas Bachet for being my pleasant mentor and Gijs Handrix for often picking me up for lunch and discussing with me about the Monte Carlo method. Next I would like to thank to the experts I had interviewed; Richard Kerkdijk, Rieks Joosten, Cor Verkoelen and Dick Welfing. They did give me much insightful information for my thesis from practical perspectives. I also would like to thank to Marijn Janssen, my chairman, and John Groenewegen, my second supervisor, for your useful comments and scientific feedbacks. I also would like to thank to Joop Koppenjan for discussing about multi-actor network.

Besides from people mentioned earlier from TU Delft and TNO, thousand thanks to my beloved family (my mom, dad and lovely sister). Once my mom said that *the best thing she can give me is education.* I thought she was right – if I have good education, I can get more education and any other things by myself. Now I think she was wrong. There are two best things I received and/or have always been receiving from her; one is education; the other is love. They have always been in my heart and I know I have been in theirs as well. Even though I learned how to quantify benefits of information security investment, I cannot quantify how much I feel grateful being a small member of this family. Great education and their love is a very important base of my thesis accomplishment. Thanks for their love, supports and motivating conversations from a far away beautiful Thailand.

Last but not least, thanks to my friends, MOT classmates and lovely housemates for supporting when I needed, for cheering me up when I was down, for cooking for me when I did not have time, for chitchatting when I was bored, for even joining me to parties when I needed a break from this thesis, and for giving me advices when I faced some difficulties in thesis or in life.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

In the first chapter, the general background information of the research is explained, followed by the problem statement. Then the research questions, the scope, and the methodology of the research are pointed out. Afterwards, the outline of this Master thesis report is presented.

1.1 GENERAL BACKGROUND

Over the last decade, information technology (IT) has become one of the success factors for many companies. Consequently, companies invest financial resource in their IT infrastructure to improve its connectivity and therefore enhance their productivity (Humaigani and Dunn 2004). Moreover companies make use of Internet for their competitive advantage because Internet enables globally access information. According to ITU research in 2007, the percentage of Internet users during 1997 and 2007 has increased from 31% to 62% in developed countries (ITU 2008). Due to the increasing interconnectivity, the number of security breaches has as well exponentially increased reported from CERT (Cavusoglu, Mishra and Raghunathan 2004). The Information Week and PricewaterhouseCoopers reviewed that only viruses and hacking breaches caused about $1.6 trillion lost worldwide (Denning 2000). As a result, information security has become crucial for a business in order to prevent those losses.

Fear, Uncertainty and Doubt (FUD) strategy has been an approach for security investment for years (Berinato 2002); however, projects aimed to improve information security is not approved easily under the financial constraint, and need to be acceptable in economic terms. Companies could not and/or should not treat spending on information security as a pure spending, but as an investment (Bojanc and Jerman-Blažič 2008). Additionally, companies would not want to spend too little as well as too much on information security investment (Anderson 2001; Schneier 2004; Anderson and Schneier 2005). Therefore, a more rational approach to analyse security investment is needed. Another approach besides FUD is the cost effective analysis which is based on the deploying cost (Cavusoglu, Mishra and Raghunathan 2004). This approach tries to achieve the most benefit an investment can get with a certain amount of budget provided. It does not quantify the benefits, simply still treat the security investment as a pure spending and does not show how much the company should invest. Another approach employs indirect estimation of losses from IT-security breaches, for example the loss in market value resulted from security breach announcements (Cavusoglu, Mishra and Raghunathan 2004). It does not help to clarify which technology should be used and how much budget should be invested. The last approach is the cost-benefit analysis. The risk framework is applied to identify the potential risks derived from expected losses and their probabilities and then calculate the expected loss (Cavusoglu, Mishra and Raghunathan 2004). The Return on Investment (ROI), the Net Present Value

(NPV) and the Internal Rate of Return (IRR) are the most common means for assessing an information security investment (Richardson 2008).

According to the CSI Computer Crime and Security Survey 2008, one of the most well-known and used methods to assess information security investment is the ROSI, return on security investment, which has been developed for years to fulfil the need of security managers. The ROSI or ROISI, return on information security investment, is adjusted from ROI. The fundamental concept is to compute the differences between the damages of IT-security incidents with safeguards and without safeguards, compared with the cost of safeguards as shown in the following formulas (Bojanc and Jerman-Blažič 2007).

$$ROI = \frac{Benefit_{safeguard} - Cost_{safeguards}}{Cost_{safeguards}}$$

$$ROSI = \frac{ALE_{withoutsafeguards} - ALE_{withsafeguards} - Cost_{safeguards}}{Cost_{safeguards}}$$

Benefits from safeguards can be computed by the savings from the Annual Loss Expectancy (ALE). More information about the ROISI approach as well as the NPV and the IRR can be found in chapter 3. When investigating the losses caused by IT-security incidents, there are two main types of losses. One is the direct cost which is physical damage to IT infrastructure, the repairing costs, cancelling appointments and deliveries, which cause loss of revenue, and regulatory penalty. The other is the indirect cost which indirectly impacts business such as lost productivity, reputation loss, company image and customer satisfaction (OCC 1998; Chan 2001; de Bie 2005; Shaw 2005). In 2008, Kim, Lee and In conducted a research and established a hierarchical structure of all major affecting factors for effective security safeguard selected by using analytic hierarchy process. The four main factors representing losses caused by IT-security incidents are lost productivity, public reputation loss, regulatory penalty and lost revenue (Kim, Lee and In 2008).

Even though, there are a considerably growing number of studies in the field of ROISI recently, applying ROISI knowledge is still problematic. The straightforward ROISI needs several variables to be estimated and results in fixed values (Lockstep 2004). One major problem is to reasonably estimate losses resulted from IT-security incidents (de Bie 2005). The likelihood of the IT-security incident occurrence and both the direct and indirect costs of the IT-security incidents are very difficult to forecast. Moreover there exists inevitable uncertainty in the IT world. Overall, it is proposed that there is a necessity for a better way to assess an information security investment that also deals with uncertainty.

1.2 Problem Statement

Failure of information security in terms of Confidentiality, Integrity Availability and Accountability (CIAA) may result in many negative consequences such as loss of revenue, penalty, lost productivity and reputation loss. As a consequence, many companies invest to develop its information security system and maintain its effective information infrastructure. There are several major problems in the area of ROISI. First, an information security

investment may need to strike with other business opportunities for resources (Conrad 2005) especially in financial crisis. Therefore it is beneficial to value information security in numeric terms and approaches should be consistent with ones used in other business investment opportunities for decision makers.

Next, many information security models trust in expert estimation (Conrad 2005), because the benefits of information security derived from less expected losses are difficult to measure. One expert may think that a certain incident would cause a significant risk, while the other believes that it can be negligible. Next to this, not only is little information about an IT-security incident available, but also this information is generally not applicable for an individual company to use. Many information sources available and accessible are collected from surveys filled in by a variety of companies (different size, industry) in a country. For that reason, a company should not use those statistics for its company because of several reasons, for example the likelihood of IT-security breach occurrence in software industry would perhaps greatly differ from one in health service industry. Therefore it is necessary to establish a better model supporting experts to make reasonable estimates. However after exploring literatures about the return on information security investment, it is concluded that there exists not such a model.

Lastly, the experts' educated guesses have to unavoidably deal with significant uncertainty. Many IT-security modelling variables such as vulnerability, likelihood of IT-security breach occurrence, impact of damage and effectiveness of mitigations involve high uncertainty (Conrad 2005). So many scenarios may occur. As a result, a single expected estimate for a modelling variable will fail to capture large uncertainty in IT-security environment (Conrad 2005). An approach, that takes into account uncertainty and reproduces the return on information security expenditure as a probability distribution, is favourable.

As a result, there is a need for a better model to depict the relation between IT-security incidents and their negative consequences in order to conduct a more powerful cost-benefit analysis that deals with uncertainty in the real world of information security. This research explores a number of earlier developed models and tools that can be used to quantitatively assess information security within a company as well as the gap between its concept and business use, and to propose an enhanced model and tool for ROISI which evaluates value of security in numeric terms and deals with uncertainty as well.

1.3 Research Question

The main objective of this research is to develop a quantitative model for return on information security investment focusing on lost revenue and regulatory penalty. Therefore the main research question to be answered in this thesis is:

In which way can the relation between IT-security incidents and their impacts be modelled to conduct the quantitative cost-benefit analysis for information security investment?

To reach the objective of establishing such a methodology for conducting the cost-benefit analysis for information security investments in organizations, the following sub-research questions need to be answered:

- What is information security and what is its role in organizations?

- What is ROISI and what is its existing approach to execute ROISI?
- What is the role of ROISI in the security risk management?
- Which methods are available to quantitatively assess information security risks?
- How should uncertainty be handled?

1.4 RESEARCH SCOPE

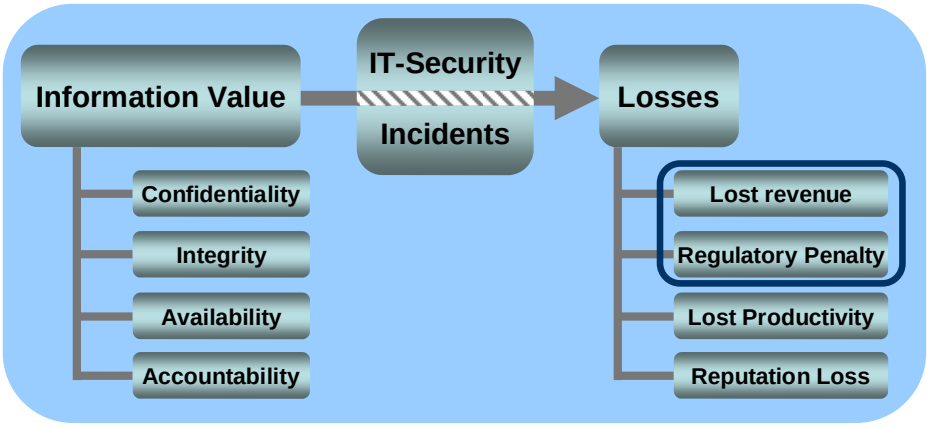


Figure 1: The business losses from IT-security incidents

The scope of the research focuses on explorative establishing a model for assessment of information security investment. This research concentrates on financial losses which are lost revenue and regulatory penalty (therefore lost productivity and reputation loss are out of scope). The research analyses different assessment approaches for security investments. This research examines existing models and tools for ROISI together with ones related to ROISI model such as Business Impact Assessment (BIA), Asset Classification (AC) and Risk Assessment (RA). The implementation gap, which is the gap between the outcome from existing risk analysis and risk assessment tools and the preferred inputs from the improved ROISI tool, is investigated. Therefore the security risk management procedures are analysed. Then the quantification approach for ROISI is developed. This research explores several techniques dealing with expert estimation and uncertainty. After a complete model is developed, a generic tool for assessing information security expenditures that generates the numeric result to support decision makers is built up. At the end, an evaluation is performed by interviewing experts about the model and the developed tool.

Due to time availability and technical complexity, the scope of the research does not include developing a risk profile, Business Impact Assessment and Asset Identification. Finding out statistical data about information security risks from the likelihood and the impact of IT-security incidents is out of scope as well. Additionally identifying the way how a company should select a suitable strategy to cope with risks is out of scope. In the research, it is assumed that a company selects the risk-mitigation approach as its strategy when using the model and the tool. In other words, the company already decides that it is going to build information security controls to mitigate its risks. Then the company would like to conduct a cost-benefit analysis to assess return on the investment. Lastly, the scope does not include

analysing how the tool or the application is used in practice. This means that actor behaviour or strategic behaviour using the application is not analysed.

1.5 Research Methodology

Methodology

The approach of this research is illustrated in the figure 2.

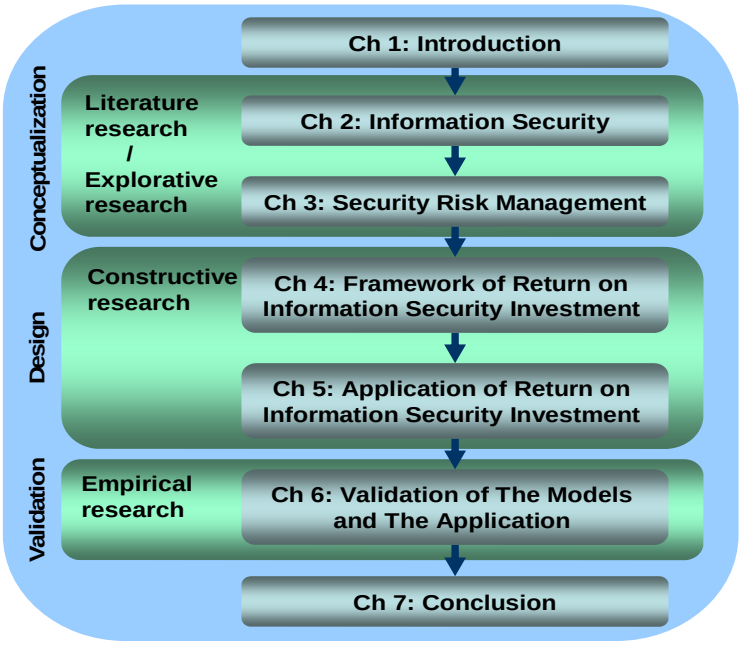


Figure 2: The research methodology

The research methodology includes three main stages in order to complete the research. The *first stage* is to explore current theoretical knowledge about ROISI as well as other relevant knowledge and to gather available tools within and outside TNO. Literature study was used since there are a number of meaningful researches both directly and indirectly related to the ROISI with different approaches. Unstructured interviews were conducted to key practitioners in order to explore the topic and understand business interests and expectations from ROISI and other relevant issues. These people were selected due to two reasons. First, they are the ones who have had the need to use the ROISI tool so they can identify problems as well as they may have high motivation to support the project process. Second, they will be the ones using it so they can identify expectations from business. From this stage, general information is clarified. Then more detailed literature according to several specific problems was further reviewed. Information about information security and security risk management was explored.

In order to develop a generic model and new tool, the *second stage* consists of data analysis, model and tool development. All important knowledge, available ROISI tools and other accessible ROISI-related tools possibly from both outside and inside TNO ICT were analyzed.

With all empirical information collected and theoretical understanding, model and tool development was conducted, presented in chapter 4 for the model development and in chapter 5 for the tool development.

In order to evaluate the outcome of this research and conclude the research project, the *third stage* is used to test the model and tool by several practitioners (approximately 3-5 persons) together with us. The people were chosen owing to, their expertise, convenience reason and human resource availability. Besides they will be the ones that are going to use it. For data gathering, a semi-structured interview was used and the conclusion was prepared.

THEORETICAL FRAMEWORK

This research will be conducted under the framework illustrated in the figure 3.

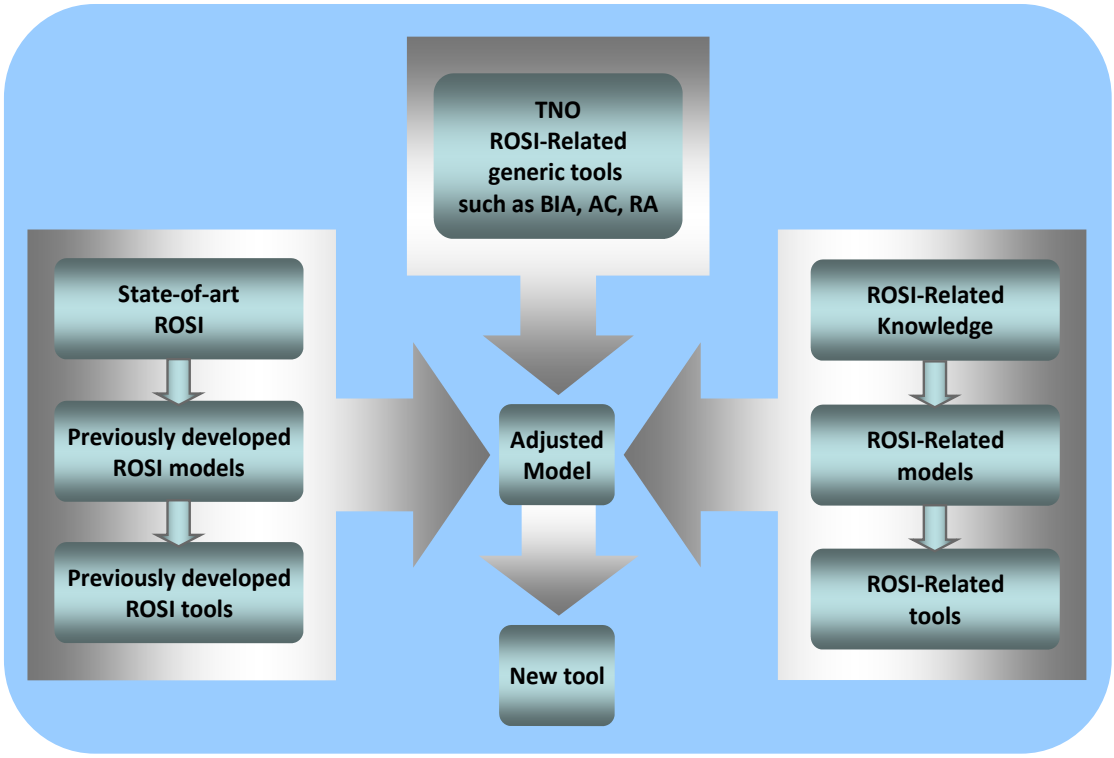


Figure 3: Framework of the design research

The research assumes that there are a number of ROISI and ROISI-related models which have been developed from potential knowledge. In order to develop a new tool to implement ROISI, it is best to make use of TNO existing ROISI-related generic tools such as Business Impact Assessment, Asset Classification and Risk Assessment tools with the combination of the existing ROISI tool; however, the interfaces between TNO tools and ROISI tools as well as other extra interests will need additional knowledge.

1.6 THESIS OUTLINE

The outline of this master thesis consists of three main sections. The first section is literature study. It is composed of general knowledge about “Information Security” in chapter 2 towards “Security Risk Management” in chapter 3. The second section is modelling and developing the tool. With the result from all the literature studies, an extended model can be constructed as described in chapter 4 “Framework of Return on Information Security Investment”. After a model is developed, an application is built based on the model as presented in chapter 5. The third section is the empirical research explained in chapter 6 “Evaluation of the Models and the Application”. Lastly, in chapter 7 the conclusion and some recommendation for further researches are described.

CHAPTER 2: INFORMATION SECURITY

Security is "the quality or state of being secure – to be free from danger". This can be considered from different layers (Whitman and Mattord 2008):

- **Physical security:** to protect physical objects from unauthorized access and/or misuse,
- **Personal security**: to protect individuals who are authorized to access the system,
- **Operations security**: to protect operations,
- **Communications security**: to protect communication media and contents,
- **Network security**: to protect networking elements, links and contents,
- **Information security**: to protect information assets.

This research focuses on the information security. In this chapter, in order to understand the component of the ROISI within the whole picture of the information security, the definition, the characteristics and the main components of information security are presented. Then lastly the need of security from both business and technical view is described.

2.1 WHAT IS INFORMATION SECURITY?

Information security is the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information (Whitman and Mattord 2008). The key concept to protect the information assets and its relevant systems from IT-security incidents are policy, education, and technology. There are several existing models explaining information security. The most well-known one is the CIA triad or CIA triangle showed in figure 4. Over 20 years, it has been used as the standard of information security based on the utility of information, which consists of confidentiality, integrity and availability.

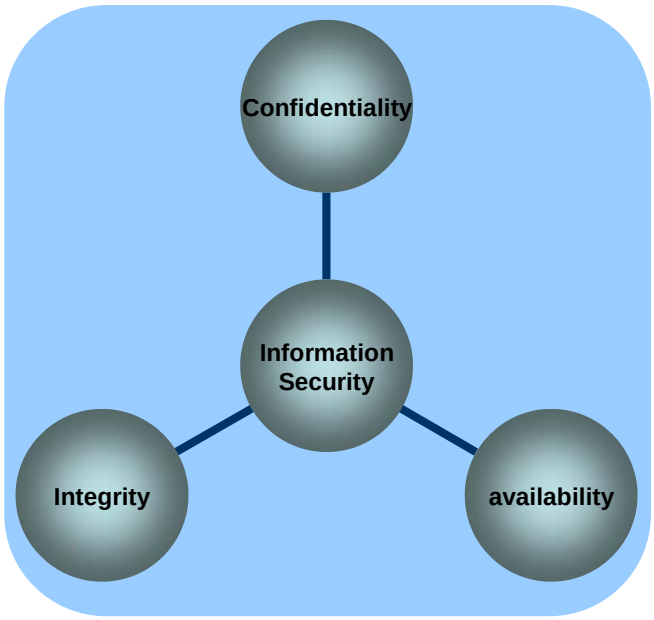


Figure 4: The CIA triangle

The CIA triangle has been extended with a list of important characteristics of information in order to address the complexity of the present information security situation. This is presented in next section.

IMPORTANT CHARACTERISTICS OF INFORMATION

The information has its value which is derived from its characteristics. If the characteristic of information alters, the value will either raise or decline. Moreover the level of information's value from the characteristics also depends on the situation and environment. Please note that there is no common agreement about the terms used in the security literature. The followings are the important characteristics of information (Whitman and Mattord 2008).

2.1.1.1 Confidentiality

Confidentiality is defined as ensuring that information is accessible only to those authorized to have access (British Standard_7799 1996). In other words, confidentiality is the state of preventing disclosure to not permitted individuals or systems (Whitman and Mattord 2008). Confidentiality of information makes sure that only the authorized can access information. If unauthorized individuals or systems can access information, the confidentiality will be violated. As a result, the value of information is lessened. Confidentiality becomes very important when it relates to personal information. To prevent a confidentiality breach, some IT-security measure can be implemented for instance information classification, secure information storage, application of general security policies and education of IT officers and end users.

2.1.1.2 Integrity

Integrity is defined as safeguarding the accuracy and completeness of information and processing methods (British Standard_7799 1996). In other words, integrity is the state of being whole, complete, and uncorrupted (Whitman and Mattord 2008). If information is corrupted, damaged or disrupted from its original state, the integrity of information is breached. This can occur when the information is compiled, stored, or transmitted. In 2008, the most frequent attack is a virus reported by the CSI Computer Crime and Security Survey (Richardson 2008). The main purpose of most viruses is to corrupt data. Two major algorithms to detect this are seeking changes in the size of the file and file hashing. File hashing algorithm converts the value of bits in the file into a single number called a hash value, which is unique for any combination of bits in the file. It shows that the integrity is breached when the computer system runs the same hashing function and the result differs from the one posted for the file. Not only the virus attack does this result in an integrity breach, but also noise can bring the same result when transmitting data. The redundancy bits and check bits can be used to ensure the integrity.

2.1.1.3 Availability

Availability is defined as ensuring that authorized users have access to information and associated assets when required (British Standard_7799 1996). In other words, availability is the state of being able for authorized user or another computer system to access to information without interference or obstruction and in a required format (Whitman and Mattord 2008). In other words, the information is ensured to be available to a user when (s)he needs it in the correct format. The availability seems to be the most basic characteristic, but very important one. In some circumstance, compliance requires an organization to address availability.

2.1.1.4 Accountability

Accountability is the state of being able to trace unambiguously an action of an entity on the system uniquely to that entity (NIST 2002). It is usually ensured by means of logging. In general some kind of identification should be performed at the beginning (ISO/IEC TR 13335-1 1996; Joshi, Aref, Ghafoor and Spafford 2001; Yskout, Heyman, Scandariato and Joosen 2006).

In order to ensure confidentiality, integrity, availability and accountability (CIAA), several control methods could be implemented. The major ones are identification, authentication and access control (IAA). For example, authentication is the state of being genuine or original, rather than a reproduction or fabrication (Whitman and Mattord 2008). In other words, authentication confirms that the information indeed is the same as when it is created from the stated source, placed, stored and transmitted as it is said to be. Some common attacks for authentication are E-mail spoofing and phishing. E-mail spoofing is the process that sends a modified E-mail message, while phishing is a means to acquire confidential

information by pretending to be another person or organization. This type of control method is used to ensure integrity of information.

Another model developed in 1991, the McCumber Cube, has become an approach frequently used in information security. It is depicted as a three dimensional Rubik's Cube for establishing and evaluating information security. The three dimensions are desired goals (confidentiality, integrity and availability), information states (storage, transmission and processing) and Safeguards (policy and practices, human factors (or education) and technology) as illustrated in figure 5. Each of these 27 cells addresses the importance issues such as availability, storage and policy when implementing information security (Whitman and Mattord 2008).

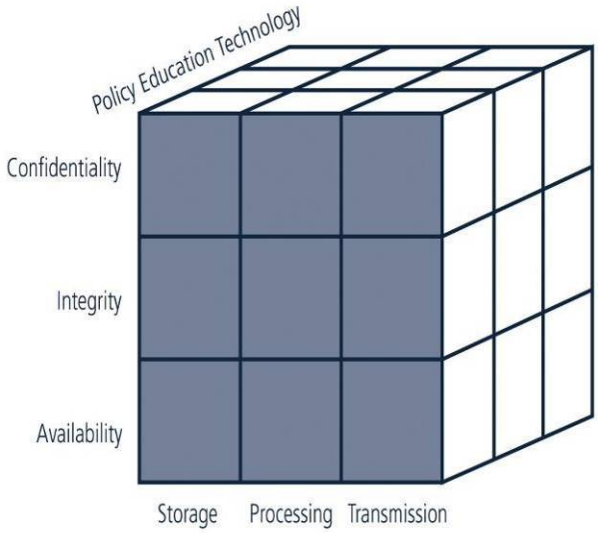


Figure 5: The McCumber Cube taken from (Whitman and Mattord 2008)

COMPONENTS OF AN INFORMATION SYSTEM

An information system is divided into six components namely hardware, software, data, people, procedures and networks (Whitman and Mattord 2008). All these components facilitate information in any information state. (The literature from Michael E. Whitman and Herbert J. Mattord in 2008 is used in the 2.1.2.1 – 2.1.2.6.)

2.1.1.5 Hardware

The functionalities of hardware are to install software, to store and transmit data, to provide interfaces to enter or remove data from the system. Therefore the security methods applying to protect hardware are locks and keys, and control access to physical components. Nowadays the percentage of laptop theft incident is ranked at the third after virus and insider abuse. In many cases, the value of information inside is much higher than the value of the laptop lost.

2.1.1.6 Software

Software includes applications, operating systems and command utilities. “Software is perhaps the most difficult information system component to secure”, stated Whitman and Mattord, professors in information security. This may result from an increased number of software vulnerabilities.

2.1.1.7 Data

Data is put into the system, processed, stored, transmitted and removed from the system. Data or information is the main target of the attack to the information security system.

2.1.1.8 People

People have three impacts to the information system: positive, neutral and negative. People can be trained to make the information system more secured. For instance, they can be trained to set their password hard to be copied, and not forget to logout the system when leaving their computer. They can normally use the information system. It is important to note that they are as well a threat to information security. According to the CSI Computer Crime and Security Survey in 2008, the second most frequent incident is insider abuse (Richardson 2008). Besides from malicious purpose, people unintentionally make mistakes. People remain the weakest part due to human error, unless the safeguards such as policy, education (or training) and technology are appropriately implemented.

2.1.1.9 Procedures

Procedures are instructions that specify the way to complete a task. The procedures are as important as the other components because a weak procedure can cause the whole information system to be not secured. For instance lack of authentication may bring losses to the company by unauthorized users. Moreover the training to employees about the procedure is as well crucial. This is because procedures can help to reduce human error when employees are trained to properly follow the procedures.

2.1.1.10 Networks

Networks support an information system to connect each other both locally by Local Area Networks (LANs) and globally by Internet. Information security faces a new challenge that it has increasingly become important to provide network security as well to secure information. Note that in some literatures for instance Master thesis from Cas de Bie in 2005, they include networks into hardware component.

The next section presents the business need for information security together with threats to information system.

2.2 THE NEED FOR INFORMATION SECURITY

Information security guards the information system together with information placed in the system from IT-security incidents.

BUSINESS NEEDS

For a business, information security has several main functionalities such as protecting information, enabling the business to operate normally, providing a safeguard platform for applications and guarding technology assets (Whitman and Mattord 2008). Especially in IT-based businesses, these functionalities are of importance as one of the keys to ensure business success. In the following sub-section, the main functionalities of an information security system in business are explained. (The literature from Michael E. Whitman and Herbert J. Mattord in 2008 is used in the 2.2.2.1 – 2.2.2.4.)

2.2.1.1 Protecting information

As mentioned earlier, the value of information depends on its characteristics and the circumstance it is present in. Protecting information in this case means to remain confidentiality, integrity and availability of information. Additionally, not only does data or information stored need to be protected, but also data that is transmitted through network or executed in any application should be protected as well. Business needs to give proper data safeguards through information security system to assure its business value derived from its information value.

2.2.1.2 Enabling the business operations

Information security is implemented to ensure business' ability to function effectively and efficiently. Actually implementing information security has to do with management, which is setting up policies and enforcement, more than with technology. To concentrate on the security need, we should address it in terms of business impact instead of technical problem.

2.2.1.3 Providing a safeguard platform for applications

IT-based companies should provide an appropriate secured platform for business' applications. Many of these applications are parts of the infrastructure such as an operating system, an e-mail application and a communicator.

2.2.1.4 Guarding technology assets

Information security services must be placed to protect technology assets in organizations. These services should be based on the size, scope and interests of the organization. Furthermore when the organization grows and the existing technology solutions can no longer support the changing needs, more appropriate security programme must replace the old ones.

Earlier the internal business needs for information security are explained. Next IT-security incidents from both inside and outside business are described to address the source for the need of information security.

THREATS

A threat is an object, person or other entity that represents a constant danger to an asset (Whitman and Mattord 2008). The 2008 CSI Computer Crime and Security Survey is one of the most well-known researches in the area of information security (Richardson 2008). It has been conducted for the last 13 years and gets usually quoted. The respondents are computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities. The survey shows that 43% of the 517 organizations had been threatened by IT-security incidents and all these incidents caused about $288,618 losses on average per respondent that year. Surprisingly and fortunately for all of us, the number of information security incidents has been decreasing over the last years. The following graph illustrates the percentage of the 433 respondents threatened by various types of information security incidents between 2004 and 2008.

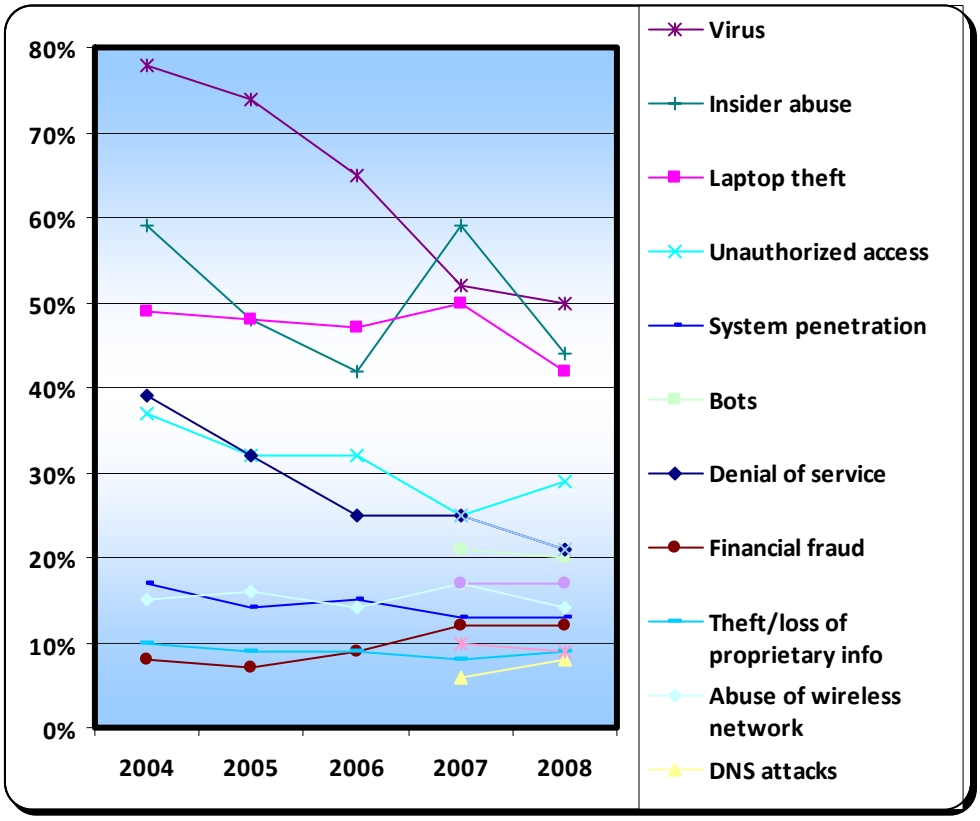


Figure 6: Percentages of major incident types (information taken from the 2008 CSI Computer Crime and Security Survey)

Virus, insider abuse, laptop theft, unauthorized access, system penetration, Bots, Denial of service, financial fraud, theft/loss of proprietary information, abuse of wireless network and

DNS attacks are the major information security incidents. This research does not focus on the technical details of IT-security threats because it is out of scope of this thesis. Each organization should prioritize the information threats based on its security situation, security/risk strategy and the exposure level of assets.

The next section explains how a company should manage its security risks which can be considered as parts of inputs for the model of ROISI.

CHAPTER 3: SECURITY RISK MANAGEMENT

"Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions." taken from (NIST 2002).

Therefore risk management is the overall process employed to identify, control and reduce the likelihood and the impact of IT-security incidents to an accepted level as *"Risk is a function of the **likelihood** of a given threat-source's exercising a particular potential vulnerability, and the resulting **impact** of that adverse event on the organization."* taken from (NIST 2002).

On the other hand, uncertainty is *"the state of lacking certainty"* or in statistics *"the estimated amount or percentage by which an observed or calculated value may differ from the true value"* (Dictionary.com Retrieved July 17, 2009). Two different types of uncertainty (Vose 2000) are uncertainty due to variability in a population and uncertainty due to a lack of knowledge. These two terminologies of risk and uncertainty are employed in the security risk world.

For the clarification, in the economics world, a well-known economist Frank Knight distinguished ***risk*** as it is ***measurable*** and ***uncertainty*** as it is ***unmeasurable***. He also uses the terms objectivity probability and insurability linked with risk, while subjectivity probability and uninsurability linked with uncertainty (Knight 1921). However please note here that there are many different definitions of uncertainty and risk in literature. For instance, in contrast with Knight, the word "risk" is generally used in public referring to any type of uncertainty with the unfavourable outcome. In this report, we use the terminologies of risk and uncertainty from the security risk world.

In this chapter, the processes in the security risk management are presented and explained.

3.1 SECURITY RISK MANAGEMENT PROCESS

Derived from the standard definition of risk presented earlier, the typical risk formula is accepted as follows (NIST 2002):

$$Risk = Impact * Likelihood$$

However when looking into the security risk management process, there are several different methodologies of risk management process found from scientific research as well as standards and guidelines reports such as the ISO 27000 series and NIST publications during the literature study phase. Most of them share similarities while slightly differing from each other. This research combines the similarities, compares differences and analyses and proposes the general security risk management process.

Generally, it consists of several major steps namely, risk analysis, risk assessment, strategy selection, cost-benefit analysis and implementation. However security risk management process is a continuing process meaning that even after implementing phase, there is a loop back to the first phase so as to evaluate the recently-implemented round and then compare the current level and the desired level for the next round. The following figure illustrates the flowchart of security risk management process (British Standard 7799-2:1999 1999; Alberts and Dorofee 2002; Butler 2003; ISO/IEC 27001:2005 2005; Peltier 2005 ; NIST Special Publication 800-100 2006; Mellado, Fernández-Medina and Piattini 2007; Kim, Lee and In 2008; Buck, Das and Hanf 2008; Whitman and Mattord 2008; Bojanc and Jerman-Blažič 2008). (All the literatures are used in the other sections in this chapter.)

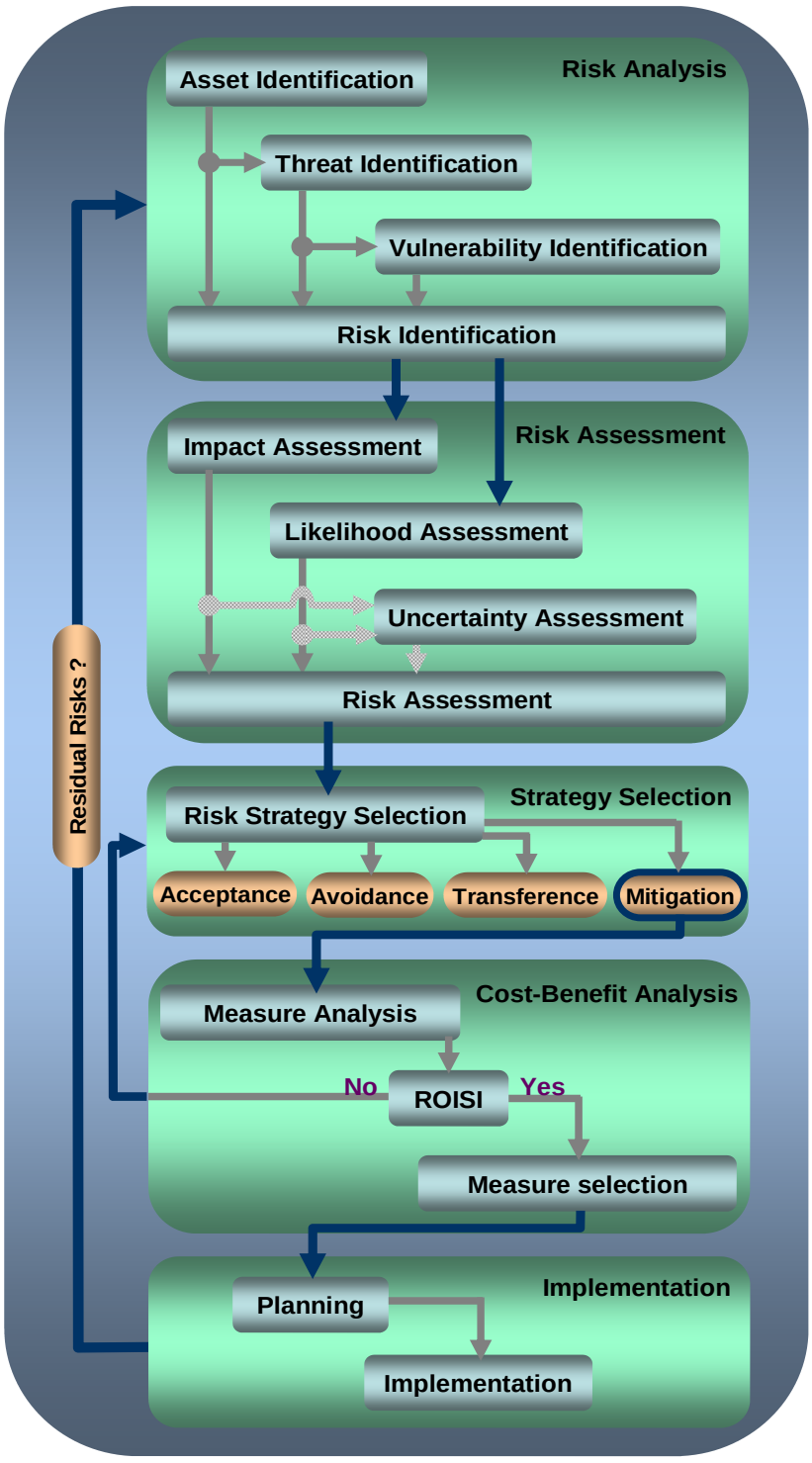


Figure 7: The flowchart of security risk management process

Please note here that the uncertainty assessment part in the security risk management model is added from most literatures. This is because not only the likelihood and the impact

have an influence on the risk assessment, but also the uncertainty of both elements does have a large impact as well. More information can be found later in this chapter.

In order to build a quantitative model for information security investment, the proposed approach is divided into five phases. First, assets, threats and vulnerabilities of the IT systems are identified in the risk analysis. Second, based on the result of risk identification, a quantitative method for risk assessment in terms of impact, likelihood and uncertainty is described. Third, not only do companies mitigate risk they face, but also they can select other options they have which are to accept, to avoid, and to transfer risks. Fourth, an approach used to assess the investment should be applied in order to reduce risk by an information security investment. In this study, the cost-benefit is used to financially verify the benefit from the measure investment. If the return of the investment is not high enough or even makes losses, decision makers need to redo the strategy selection phase. Fifth, the implementation phase is conducted and then the evaluation part for residual risks gives a loopback to the first phase. Before starting with the whole process, some clarifications are needed to be pointed out. Many types of risks can affect a company: *strategic risks* relating to the political and social environment, *financial risk* relating to the money market and interest rate and *operational risk* relating to the business processes. This research focuses on information security risk as part of the operational risk.

3.2 Risk Analysis

The objective of risk analysis is to identify and measure the risks in order to inform the decision-making process. Risk analysis needs the data about information assets as well as assets of IT system in the organization, threats to which assets are exposed and vulnerabilities of the IT system that threats may exploit as shown in figure 8.

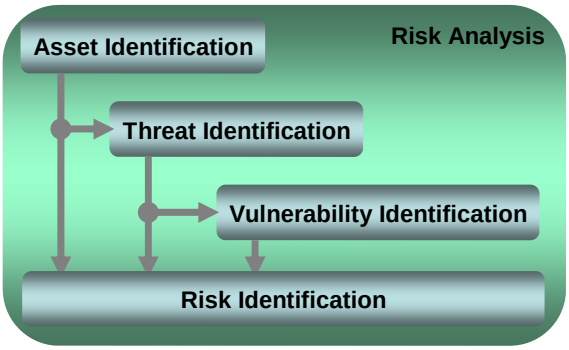


Figure 8: Risk analysis

ASSET IDENTIFICATION

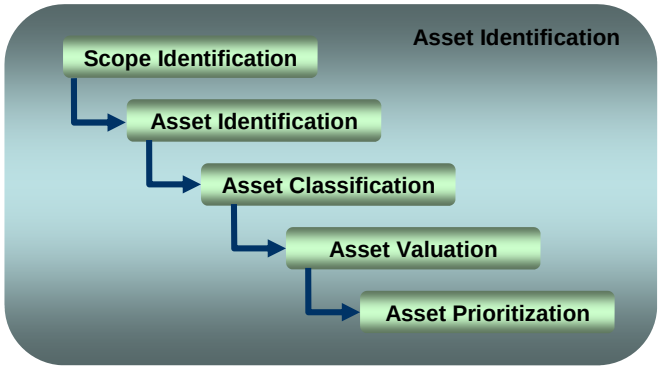


Figure 9: Risk identification

Business process highly depends on information assets in today's business. Before identifying the organization's assets, the boundaries of the IT system should be first identified. Then classification is taken place. Derived from the common components of information system as presented in chapter 2, the classification of system-related information is usually as follows (NIST 2002):

- Hardware
- Software
- System interfaces – internal and external connectivity
- Data and information
- Persons – IT personnel and IT users
- System mission – the processes performed by the IT system
- System and data criticality – the system's value or its importance
- System and data sensitivity – the protection level to remain confidentiality, integrity, availability and accountability

Normally the classification should be specific enough to determine the priority level. This is more important than the way the company chooses to identify assets. It is necessary that the classification be *comprehensive* and *mutually exclusive*. Therefore all information assets must stand in the list somewhere (comprehensive) and each information asset must fit in only one category. An example of the classification list is confidential, private and public. The classification can have more levels; this depends on the environment of IT system of a company.

After specifying the scope of the analysis, identifying assets and classifying them, information assets as well as assets of IT system are evaluated based on their value they possess. Tangible assets from physical infrastructure such as servers, workstations and network and from software parts are easier to be measured its value than intangible assets such as business data, organization knowledge and the intellectual property information stored

(Bojanc and Jerman-Blažič 2008). The weighting criteria can be applied for asset valuation. Two very different examples of the criteria are as follows:

- Critical level to the company success: This criterion refers an asset's importance to the company mission or objective since business process depends on information. Examples are impact to revenue, profitability and public image.
- Value to adversaries: This criterion assesses the worthy level to a company to know what the competition is up to.

This valuation may use a numeric process (shown below) as well as linguistic one (critical, high, medium, low and insignificant). The scores of criteria range from 0.1 to 1.0 recommended by NIST SP800-30. The more number of different classes the criteria have, the more precise but the more time-consuming the determination of a proper class.

Table 1: A sample of weighted value for information assets importance

Information Asset	Criteria 1: Impact to revenue	Criteria 1: Impact to profitability	Criteria 1: Impact to public Image	Weighted Score
Criteria Weight	30	40	30	
Information A	0.8	0.9	0.5	75
Information B	0.4	0.5	0.3	41
Information C	0.4	0.4	0.9	55

Table 1 shows an example of the asset valuation template; the result of this table supports analysts to conduct the asset prioritization. After this, the assets are usually prioritized in order to support the company to concentrate on the most critical ones. The information assets can be prioritized from the weighted score. As a result from this sample, information A is the most important for the company and followed by information C and information B respectively.

THREAT IDENTIFICATION

The second step of risk analysis is threat identification. A threat is any probable cause resulted in unwanted impact and exposes information assets (NIST 2002; Bistarelli, Fioravanti and Peretti 2006). Similarly to asset identification, threats should be identified and prioritized. Before selecting any IT-security measure or even establishing security policy, threats a company faces must be clearly identified. The threats have different target assets. The following tree explains the different types of threats.

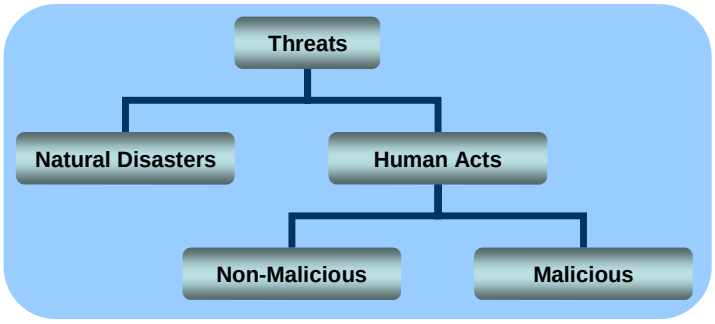


Figure 10: Threat classification

There are different types of malicious humans act threats as for objective, access, resource, expertise and risk (Schneier 2004). Attackers use this type of threats for various reasons such as gaining competitive advantage, personal satisfaction, financial gain, revenge, spying and violence (Bojanc and Jerman-Blažič 2008). In most cases, an IT-security system is designed to control the malicious human threats such as virus, insider abuse, laptop theft, unauthorized access, system penetration, bots, denial of service, financial fraud, theft/loss of proprietary information, abuse of wireless network and DNS attacks. According to the CSI computer crime and security survey, financial fraud is the most expensive computer security incident, while virus is the most frequently occurring in 2008. The financial consequences of cybercrime are considerable, although the loss estimates have dropped for the five consecutive years. Fortunately, it is stated in the survey report that *"the attacks are less imaginative than what is currently theoretically possible"*. Interpretably, it is not so difficult to identify threats nowadays.

To identify threats, many common existing methods can be used such as developing checklists, examining historical data internally and externally and brainstorming (Whitman and Mattord 2008). The combination of methods is often used. After this, threats should be assessed its potentials to threaten the company and prioritized due to its danger and/or an amount of expenditures needed.

VULNERABILITY IDENTIFICATION

Vulnerability is a defect or weakness in information asset, security procedure, technical design or control that a threat may exploit on purpose or even accidentally to breach security system. Most IT-security incidents are caused by vulnerabilities in software. Statistics from CERT in 2007 showed that the number of vulnerabilities has increased at an alarming rate from 171 in 1995 to 8064 in 2006 (CERT 2007). Vulnerabilities are possibly not only technical errors, but also human factor when users share passwords or use weak passwords, open untruthful e-mail, visit fraudulent web sites, or download malicious software. Due to a growing number of open-source communities, vulnerability disclosure has become a critical concerning point whether it is more beneficial to protect information assets or disclose a means for attackers to exploit the IT system. To identify vulnerabilities, similar methods from threat identification can be applied. Nevertheless the identifying vulnerabilities process is rather subjective, which is based on the knowledge and experience of experts. Therefore it is

advisable that experts should have diverse background and brainstorm iteratively (Whitman and Mattord 2008).

Once risks are analyzed, the lists of assets, threats and vulnerabilities are constructed and used as a starting point. Next step of the security risk management process is risk assessment.

3.3 Risk Assessment

The objective of risk assessment is to support companies to assess their risk in order to help in making decision regarding strategy coping with information security risk and the needed investment in security controls. Risk assessment typically needs the data of the current situation about the impact of risk or potential loss in the organization and the likelihood or the probability of risk occurrence as shown in figure 11.

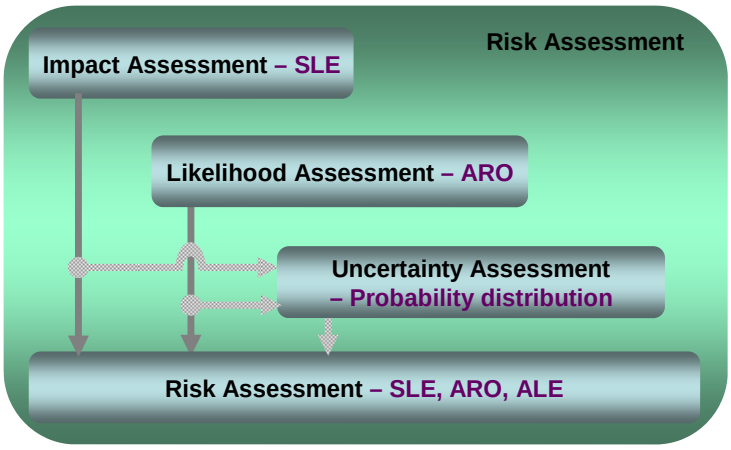


Figure 11: Risk assessment approach

Additionally uncertainty assessment can be added to compensate the expert's lack of precise knowledge and uncertainty in information security environment. There are many different methodologies for assessing risks which is described in the next section.

Qualitative and Quantitative Risk Assessment

The major approach for assessing risks can be divided into quantitative and qualitative approaches. A quantitative risk assessment attempts to assign numeric values to both impact and the likelihood of risks, while a qualitative risk assessment attempts to give relative values such as high, medium and low. The qualitative risk assessment is often conducted through questionnaires and collaborative workshops (Bojanc and Jerman-Blažič 2008).

Both qualitative and quantitative approaches have their advantages and disadvantages. The main advantage of qualitative risk assessment is that it requires fewer resources. More precise information about the impact, the probability and the investment expenditure is not needed. In some cases, companies still use FUD (Fear, Uncertainty and Doubt) strategy. This makes a quantitative ROISI not necessary; therefore, the qualitative approach will suit better for those companies. The disadvantage of the qualitative approach is that it is relatively

vague and not precise since results are derived from relative values of assets (Bojanc and Jerman-Blažič 2008). Additionally information security investment may need to strike with other business opportunities for resources (Conrad 2005) especially in financial crisis. Therefore it is more suitable to value information security in numeric terms and consistent with other approaches such as ROI, NPV or IRR for decision makers, which is the major benefit from the quantitative risk assessment. The quantitative approach enables the results more precise, while it is relatively resource consuming. With the quantitative approach, it is possible to optimally mitigate risks up to a breakeven point where the cost of security investment is equal to or less than the return of the investment.

In this paper, we focus on the quantitative methodology, which is explained further for each process in risk assessment. One of the most common analytical quantitative methods for exposure to a risk is *Annual Loss Expectancy* (ALE). The ALE is recommended by the international Information Systems Security Certification Consortium (ISC)^2. The Certified Information System Security Professional (CISSP) programme is developed by the (ISC)^2. The programme is tested and certified by 40,000 security experts. This may be because the ALE is effective in aiding security managers to estimate an expected loss from an IT-security incident. This ALE calculation needs the determination of the numeric loss regarding the impact, which is called *Single Loss Exposure* (SLE). Moreover the determination of the probability regarding the risk occurrence, which is called *Annual Rate of Occurrence* (ARO) is required as well in the calculation.

IMPACT ASSESSMENT

The impact assessment can be considered as the most problematic part of risk assessment because there are a variety of ways to assess the impact of information risk existing in literatures. The more detailed explanation is presented in a later chapter. That chapter explains the important elements of the impact of risks in information security system. However in this chapter, some basic concepts are presented. Impact assessment determines the consequence of a risk. These can include death, injury, financial loss, key agency function or service delivery, publicity, penalty and so on. Then an appropriate consequence rating is defined. From all or major damaging consequences, the determination of the numeric loss from the impact of an IT-security risk is conducted. The single loss exposure (SLE) is applied in general.

3.3.1.1 Single Loss Exposure (SLE)

The SLE is the "total" amount of lost revenue resulted from a single occurrence of the risk (NIST 2002; Tsiakis and Stephanides 2005; Bojanc and Jerman-Blažič 2008). A monetary amount is assigned to represent the company's possible loss if a threat exploits the vulnerability of the IT system supporting the company's assets. The *SLE* is sometimes a product of asset value (*AV*) multiplying with the exposure factor (*EF*) as shown below.

$$SLE = AV * EF$$

The *AV* represents the cost of creation, development, support, replacement and ownership value of an asset (Krutz, Vines and Stroz 2001) and preferably is expressed as a monetary

value of the asset. The *EF* represents the magnitude of loss or impact on the value of an asset resulting from a threat incident, and is expressed as a percentage of the asset value (Krause and Tipton 1999). An oversimplified sample from Rok Bojanc and Borka Jerman-Blažič explaining the approach is in a case when the web server has an *AV* of €50,000, and a virus incident affecting the server results in expected loss of 35% of the value, meaning that *EF* is equal to 35%, then the *SLE* has an estimated value of €17,500 as shown below.

$$SLE = 50,000 * 35\% = 17,500$$

LIKELIHOOD ASSESSMENT

Likelihood is the probability that certain vulnerability will be exploited (NIST 2002; Tsiakis and Stephanides 2005; Bojanc and Jerman-Blažič 2008). A sample from the department of Defence in Australian Government is presented in the appendix C. This sample uses a qualitative approach for the likelihood assessment and applies it to quantitative approach. In the quantitative risk assessment, numeric values are assigned to estimate the likelihood. It is essence that no matter which rating system a company employs; a company use professionalism, experience, judgment and, more importantly, use the system consistently (Whitman and Mattord 2008). In general, the Annual Rate of Occurrence (ARO) can be applied since it is one of the most applicable for information security risk assessment from our point of view.

3.3.1.2 Annual Rate of Occurrence (ARO)

When the SLE is determined for a risk to estimate the level of its potential impact, the ARO is needed to determine the risk's occurring frequency. The ARO is basically the number of times that the company rationally expects that risk to occur in one year. For example, if a virus incident probably occurs once in 2 years, the ARO is equal to 0.5.

UNCERTAINTY ASSESSMENT

The experts' educated guesses have to unavoidably deal with significant uncertainty. First of all, in order to understand uncertainty better, it is good to mention an issue of probability because generally uncertainty of input variables in a model is presented in the form of a probability distribution. Here we present two different views on probability: the frequentist and the Bayesian. The frequentist view considers the probability of an event as the relative frequency of occurrence of an experiment's outcome, when the experiment is random and well-defined. The Bayesian view considers the probability of an event as an individual's degree of belief that it will occur, given the state of information of that individual. In the context of ROISI, the Bayesian view is better fit since it is about expert estimation, or in other words it is basically dependent on his/her degree of belief.

When we understand the general two views of probability, then there are two different types of uncertainty as follows (Vose 2000):

- **Uncertainty due to variability in a population:** This type of uncertainty cannot be reduced by adding more information.

- **Uncertainty due to a lack of knowledge:** This type of uncertainty is reducible by additional information.

These two types of uncertainty often exist together in a situation; however, only variability is considered in the uncertainty assessment part. Expert estimation on variability is still in form of subjectivity probability distribution. In business environment, it is (almost) not possible to define an objective probability distribution. Many IT-security modelling variables such as vulnerability, likelihood of IT-security breach occurrence, impact of damage, effectiveness of mitigations involve high uncertainty (Conrad 2005). So many scenarios may occur. As a result, a single expected estimate for a modelling variable will fail to capture large uncertainty in IT-security environment (Conrad 2005). Simply, for major parameters involved high uncertainty the estimated probability distributions should be defined such as mean, range of the possible numeric values, distribution pattern for example uniform, triangular or normal distribution and standard deviation.

After all of these determinations of the SLE and the ARO, the final ALE can be calculated as the last process in a quantitative risk assessment.

ANNUAL LOSS EXPECTANCY OR ANNUALIZED LOSS EXPECTANCY (ALE)

Security risk can be measured from the *ALE*, which is product of the *ARO* multiplying with the *SLE* as shown below.

$$ALE = SLE * ARO$$

The *ALE* represents the annually expected financial loss of a company which can be ascribed to a threat if a company does not mitigate the risk.

For the same example, if a virus incident at the web server costs loss of €17,500 and the likelihood of this virus incident has an *ARO* value of 0.5 (meaning that it probably occurs once in 2 years), then the *ALE* value of this web server would be €17,500*0.5 = €8750 as shown below.

$$ALE = 17,500 * 0.5 = 8,750$$

After a company obtains values of the *SLE*, *ARO* and *ALE*, a risk-rating scale can be generated in order to enable a company to prioritize its risks from the value of the *ALE* as the final step of risk assessment. A simple example is shown in table 2.

Table 2: A simple sample of risk-rating scale adapted from (NIST 2002)

Risk Scale	Risk level	Recommendation
1-5,000	Low	IT-security officers must determine whether curative actions are still needed or decide to accept the risk.
5,001-20,000	Medium	Curative actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time and resources.
20,001-500,000	High	Curative measures are strongly needed. An existing system may continue to operate, but a corrective action plan must take in place as soon as possible.

Moreover there is another approach to conduct the quantitative risk assessment applied from the qualitative technique. The impact and likelihood level of a risk can be classified into several levels such as low, medium and high. Then a company can assign numeric expected loss or frequency that likely happens in one year for each level. A risk-level matrix could be developed to measure risks. The risk-level matrix can be constructed by multiplying the rating from the impact assessment and the likelihood assessment.

Table 3: A sample of simple risk-level matrix

Impact / Likelihood	Low (5,000)	Medium (15,000)	High (40,000)
High (1.0)	5,000	15,000	40,000
Medium (0.5)	2,500	7,500	20,000
Low (0.1)	500	1,500	4,000

Before moving to the next phase of security risk management which is the strategy selection, three relevant issues are presented to handle uncertainty. One is the Monte Carlo approach, another is sensitivity analysis and the other is expert opinion.

3.3.1.3 The Monte Carlo Approach

At the uncertainty assessment part, analysts may make use of the Monte Carlo method to handle uncertainty. The Monte Carlo method is defined as *"representing the solution of a problem as a parameter of a hypothetical population, and using a random sequence of numbers to construct a sample of the population, from which statistical estimates of the parameter can be obtained"* (Halton 1970). A Monte Carlo simulation can be built from the Monte Carlo method for analysts to use. The simulation basically treats an information security model as a function with a set of input parameters (for instance the likelihood and the impact of IT-security incidents) and then returns a set of projected results (Conrad 2005).

In other words, for thousands of times, the simulation randomly selects a value for each parameter and calculates the results of the model. With the Monte Carlo simulation, more information about the results is provided to support decision makers. For example, the possible distribution of output parameters and the confidence level of the results can be presented from the simulation.

However the Monte Carlo approach requires extra information from experts to describe uncertainty for several particular variables in a model such as mean, range, standard deviation, and distribution pattern for example uniform, triangular or normal distribution. Many experts are not comfortable with a single expected value, while the major problems of using the Monte Carlo approach are that they do not have information about the probability distribution and that providing extra information is very time-consuming.

3.3.1.4 Sensitivity analysis

Sensitivity analysis is *"the study of how the variation or uncertainty of the defined output of a mathematical model can be apportioned to different sources of variation of the input of the model"* taken from (Saltelli 2004). Sensitivity analysis can support decision makers to better understanding the model structure and the main sources or inputs of model output uncertainty (Ratto, Tarantola, and Saltelli 2001).

3.3.1.5 Expert Opinion

Many parts in the security risk management involve expert opinion, which is personal believe. About accuracy, Mosleh, Bier, and Apostolakis claim that the two main biases in risk assessment are systematic over- or under-estimation and overconfidence (Mosleh, Bier and Apostolakis 1988). Overconfidence is the tendency that experts give an estimate more certainty than it is justified by their knowledge. Overconfidence can be reduced by giving an expert feedback and training. Besides from giving feedback and training, disaggregation can lessen biases as well. This can be done by splitting an estimate into smaller parts so that an expert can give better estimates. Moreover it is usually preferable to combine more than one expert's opinions. Multiple experts are most likely able to provide more information than a single expert; therefore, the reliability of information may reasonably increase.

Next section explains the way a company can have to handle risks. The company can exercise information from risk assessment to choose the right strategy to minimize risks.

3.4 STRATEGY SELECTION

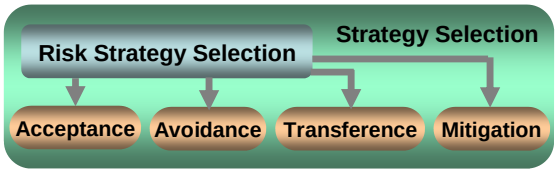


Figure 12: The risk mitigation strategy selection phase

After information security risks have been analyzed and assessed, the company continues the next step of security risk management by selecting the appropriate strategy to reduce its risks (NIST 2002). The possible strategies are as follows (NIST 2002; Tsiakis and Stephanides 2005; Bojanc and Jerman-Blažič 2008):

- **Acceptance:** Acceptance is the choice to do nothing against a risk of having threat exploiting a company's vulnerability and considers the damaging consequence as a cost of doing business. Risk acceptance can be a reasonable strategy where the cost of mitigation or transference the risk is greater than the total losses sustained (Bojanc and Jerman-Blažič 2008). Additionally, it seems reasonable as well when the ARO is significantly small. On the other hand, acceptance can be mistakenly chosen based on "*the school of fish justification*" – sharks will not come after a small fish in a school of other small fish (Whitman and Mattord 2008).
- **Avoidance:** Avoidance is the choice to avoid a risk by removing the risk source and/or consequences. This is preferably applied when the risk impact is higher than the benefit from that asset. Examples are deleting some functions in the system or even removing the whole system.
- **Transference:** Transference is the choice to shift risk to other assets, processes or organizations by outsourcing information security services, buying insurance (Böhme and Kataria 2006; Whitman and Mattord 2008), rethinking how services are offered, revising deployment models or implementing service contract with providers (Whitman and Mattord 2008).
- **Mitigation:** Mitigation is the choice to mitigate the impact of vulnerability exploitation by implementing proper information security systems or tools such as antivirus or firewall or implementing proper security policies such as access control or passwords. The mitigation strategy is considered as the primary risk management strategy (Bojanc and Jerman-Blažič 2008).

According to the result found during the literature study, there exists no standardized procedure for choosing the right risk-mitigation strategy. In general, a company should select the right strategy is based on the context it is embedded in. It is stated by Cheng and Levitt that contextual factors may influence decision making (Cheng and Levitt 2000). Moreover defining an ideal approach is not in the scope of this research. Figure 13 illustrates the main inputs, which are company objective/environment, measure identification and the results from risk analysis and risk assessment, and possible outputs for the decision making process.

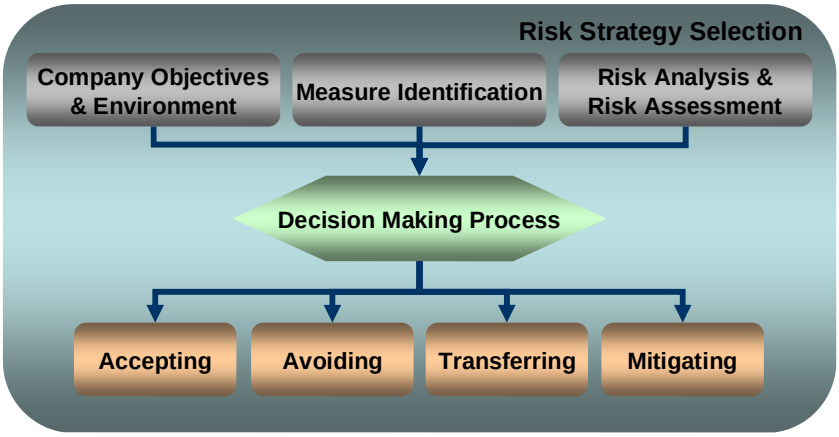


Figure 13: Risk strategy selection

In order to understand the measure identification part, the next sub-section explains different dimensions of security controls.

SECURITY CONTROLS

Companies employ countermeasures to handle threats. These countermeasures can be considered into two classifications. One consists of physical, organizational and logical controls; the other composes of preventive, detective, regressive and corrective controls (van den Berg and van der Pijl 2004; Bie 2005; Pathak 2005; Zegers 2006). (The four literatures are used in the 3.4.1.1 and 3.4.1.2.)

3.4.1.1 First dimension of IT-security measures

- **Physical controls:** These IT-security measures try to protect IT system equipments from physical threats such as malfunction, unauthorized access, physical damage and theft. Examples are gates and locks.
- **Logical controls:** These measures are aimed to protect IT software and information (or data) to prevent damage like unauthorized access, mistakes and fraud. Examples are access controls, encryption, security certificates and virus protection.
- **Organizational controls:** These measures complement the system of physical and logical controls in order to realize the security objectives. Examples are segregation of duties and security policies.

3.4.1.2 Second dimension of IT-security measures

The second classification of IT-security measures is illustrated in Figure 14.

- **Preventive controls:** The objective of these measures is to prevent IT-security threats from materializing into IT-security incidents. Examples are access control enforcement, encryption and authentication.
- **Detective controls:** The goal of these measures is to detect IT-security incidents to prevent damaging consequences from incidents. Examples of methods are audit

trails, intrusion detection methods and checksums. It is a kind of regressive controls in terms of reducing negative consequences before damage occurred.

- **Regressive controls:** These regressive measures have the goal to reduce the damaging consequences when they cannot be prevented.
- **Corrective controls:** The objective of these corrective measures is to repair damages caused by IT-incidents. It is a kind of regressive controls in terms of reducing negative consequences after damage occurred.

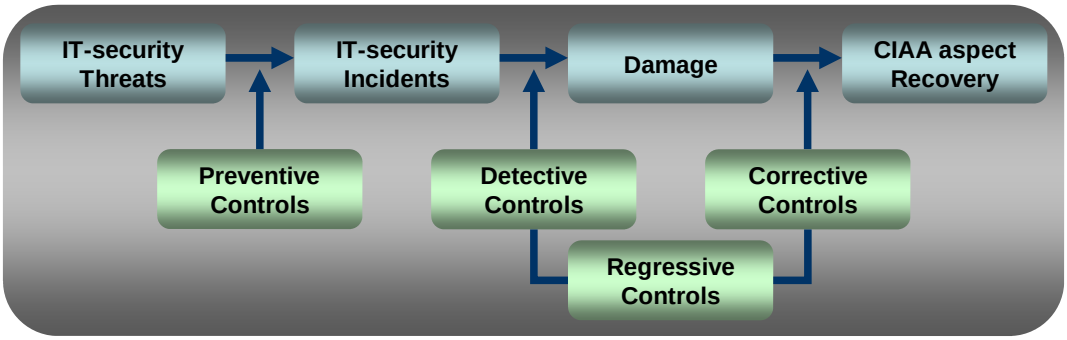


Figure 14: The impact of IT-security controls adapted from (van den Berg and van der Pijl 2004)

As shown in figure 14, preventive controls prevent a threat from developing an IT-security incident, while detective and corrective controls handle the threat materialization.

In this thesis, the risk mitigation strategy is concerned as it is the primary risk management strategy and it needs the cost-benefit analysis for information security investment, which is an important focus in this research. Previous steps in the information security risk management can be considered as inputs for the ROISI model to conduct cost-benefit analysis. In the next section, information about cost-benefit analysis is elaborated.

3.5 Information Security Investment: Cost-Benefit Analysis

When decision makers select the mitigation strategy to handle risks, an information security investment for implementing countermeasures against those risks should be assessed. The intention of the investment is to lower the impact or damaging consequences and the likelihood of IT-security incidents. Risks (Conrad 2005) can be optimally mitigated by the use of the cost-benefit analysis. The cost-benefit analysis has become the most popular metrics when applied with computer-related risks (Mercuri 2003). It is established in microeconomic and management accounting theory. There are several accepted approaches incorporating the cost-benefit analysis such as Return on Investment (ROI), Net Present Value (NPV) and Internal Rate of Return (IRR). These are used as financial metrics for quantifying the cost and benefit of information security investment. Although looking at different approaches, the expenditures of information security are similarly weighed against the estimated benefits (Gordon and Loeb 2002; Schechter 2002). Companies should consider the financial feasibility of implementing information security measures. In general, a company should make an

information security investment when the benefits exceed its costs. As a result, there is a need for a company to conduct an economic feasibility study or in other words a cost-benefit analysis. Figure 15 below illustrates the steps for conducting the cost-benefit analysis.

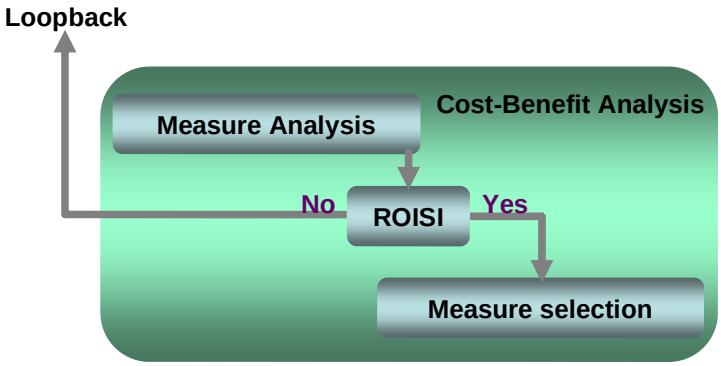


Figure 15: The cost-benefit analysis phase

After a company selects the risk mitigation as its strategy, together with measure identification step from the earlier phase the company should analyze the identified measures to evaluate their benefits and costs. Benefit is the value that a company realizes by using measures to reduce losses from a particular vulnerability (Whitman and Mattord 2008). The benefits could be in terms of how much the impact and the likelihood of IT-security incidents the measures can reduce, or in other words, a reduction in the ALE. The costs could be in terms of cost of implementation (hardware and software), cost of maintenance, cost of personnel and cost of training (Peltier 2005). With the results from the measure analysis, the company can perform the ROISI calculation by using one of the approaches mentioned or a combination of them. Despite of all these existing approaches, the ROISI has business problems. According to the ROSI report, the ROSI or ROISI limitations are as follows (ISF 2005):

- Understanding ROSI
  - ROSI is weakly defined
  - The concept of ROSI is not fully formed
  - ROSI calculations are little known or understood
- Applying ROSI
  - ROSI can be complicated to apply in a company
  - The business benefits of security can be hard to demonstrate
  - ROSI term is not generally used in business
- Calculating ROSI
  - Approaches to calculating ROSI are difficult and inconsistent
  - Data needed is often limited
  - Incident avoidance costs are hard to estimate

In the next section, each approach is explained and compared.

RETURN ON INVESTMENT (ROI) AND RETURN ON INFORMATION SECURITY INVESTMENT (ROISI)

The ROI is a well-known accounting metric for comparison of business opportunities. The ROI basically shows how much a company earns from invested money. So the ROI can support decision makers to select the possible options that have the most return. The result is a percentage of the return over a certain period of time. The ROI is calculated by the present value of accumulated net benefits over a certain time period subtracted by the initial costs of investment, then divided by the initial costs of investment as presented in the formula below:

$$ROI = \frac{Benefits - Costs}{Costs}$$

For simple example, if a new web server costs €10,000 and is estimated to generate €50,000 income over 4 years, then the ROI is 400% as shown below:

$$ROI = \frac{50000 - 10000}{10000} = 400\%$$

When applying the ROI concept into the ROISI, several parts need to adapt. The benefit can be considered as a difference between ALE without security investment and ALE with security investment as follows:

$$Benefits = ALE_{withoutsafeguards} - ALE_{withsafeguards}$$

The cost of information security investments includes the configuration costs and the operating costs. The configuration costs are normally one-time costs, while the operating costs include annual maintenance, training end-users and IT staffs. In general, the costs of safeguard implementation are rather easily defined, in contrast with its benefits. This is because an information security investment does not generate income. However it does have the impact on cost savings resulting from preventing IT-security incidents (Gordon and Loeb 2006). To calculate the ROISI, an adapted formula for ROISI from the ROI and the nature of information security is as follows:

$$ROISI = \frac{ALE_{withoutsafeguards} - ALE_{withsafeguards} - Cost_{safeguards}}{Cost_{safeguards}}$$

To illustrate this with the same previous example, the ALE of virus infection on a web server is €8750. If a company installs antivirus software, the ALE will be reduced to €3400. The configuration for antivirus software costs €1600, while the yearly operating cost of the safeguard is €450, then the ROISI in the first year is 160% as shown below:

$$ROISI = \frac{8750 - 3400 - (1600 + 450)}{1600 + 450} \approx 161\%$$

NET PRESENT VALUE (NPV)

The NPV is a financial metric for comparing costs and benefits over period of time; therefore it is well used to analyze long-term investments. The main approach of the NPV is to discount all expected costs and benefits from an investment to its present value, therefore the time value of money is taken into consideration. The NPV concept is then to compare the discounted cash flow generated in the future with its initial investment. The NVP is calculated by summing the total present value of the benefits and (operating) costs for each year over *n* periods and then deducting the initially required (configuration) costs as shown in the formula below (Neuhaus 2008):

$$NPV = \sum_{t=0}^{T} \frac{B_t - C_t}{(1+r)^t}$$

Suppose B_t is all benefits at the period *t*, C_t is all costs at the period *t* and *r* is the internal rate of discount, discount rate or opportunity cost of capital. *T* is number of years. Rational estimation of discount rate and cash flows is critical because the NPV is very responsive to these parameters (Neuhaus 2008). More information about the internal rate of discount, discount rate or opportunity cost of capital can be found in the appendix.

The decision rule is that a decision maker should accept investment opportunities offering a positive net present value because they generate a profit or the higher NPV when comparing among investment opportunities. In contrast to a positive NPV, a project having a negative NPV makes a loss. It is as well useful when a decision maker needs to compare alternatives, for example a comparison between two investments where one needs €15,000 one-time payment while the other needs €5000 for 3 years. Both investment opportunities cost €15,000 and equally generate the benefits at the same time. The decision maker should select the second because the NPV of the second higher. This is because the discounted cost of the second opportunity is lower than the first one. The company can invest the remaining money in other opportunities for a period of time.

INTERNAL RATE OF RETURN (IRR)

Like the NPV, the IRR is often used to assess and compare long-term investments. The IRR is the rate of return that makes the net present value equal to zero. In other words, the IRR is the rate at which the total present value of the anticipated cash flow is the same as the initially required investment (Neuhaus 2008).

$$NPV = \sum_{t=0}^{T} \frac{B_t - C_t}{(1+IRR)^t} = 0$$

Suppose B_t is all benefits at the period *t*, C_t is all costs at the period *t*, *r* is the internal rate of discount, discount rate or opportunity cost of capital and *T* is number of years where *IRR* is the rate of return.

The decision rule is that a decision maker should accept investment opportunities offering a rate of return greater than their opportunity cost of capital (or hurdle rate) or else the higher IRR when comparing among investment opportunities (Neuhaus 2008). The IRR is often used

especially when a long-term investment is made of which the costs radically change year to year (Bojanc and Jerman-Blažič 2008).

In the next section, the comparison of all approaches is presented in order to show their strengths and weaknesses.

THE COMPARISON AMONG ROI, NPV AND IRR

Each of these financial measures namely ROI, NPV and IRR has its own advantages and disadvantages. While the ROI presents a percentage of return of an investment over a defined time period, like the IRR it does not inform about the magnitude of the investment. So the NPV is the only approach informing about the magnitude of the project. The ROI faces a problem in the case of long-term investments because it does not consider the time value of money; therefore a decision maker would need the NPV as well to justify investment opportunities. This is because a significant characteristic of the NPV is that it presents the discounted cash value of the anticipated return and consequently the magnitude of the project.

On the other hand, the fact that the NPV is very responsive to the time value of money and the time value of money has limited information may bring disadvantage towards the use of the NPV alone. Lastly, the IRR has a doubtful assumption because it assumes that the whole period of time has the same rate of return. An expert in the field, Markus Neuhaus, mentioned that the NPV is superior, so in case of conflicting results, a decision maker should go with the NPV. This may be because the NPV is easier to use and less tendency to wrong decisions, while the IRR is founded on the reinvestment assumption.

Table 4: The comparison for all presented approaches

Approach	ROI	NPV	IRR
Magnitude	No	Yes	No
Time value of money	No	Yes	Yes
Complexity	Low	High	High
Popularity	High	Medium	Medium/Low
Comment	Less reliable than the other two approaches	Sensitive to the time value of money which has limited information	doubtful assumption: the whole period has the same rate of return

In general, the NPV and the IRR are better approaches than the simple ROI (Gordon and Richardson 2004). Practically a company should use a combination of these approaches to get a better picture of an investment (Bojanc and Jerman-Blažič 2008). This may be because each approach would need another approach to compensate its weaknesses. According to

the CSI Computer Crime and Security Survey, the ROI is the most popular approach in 2008, followed by the NPV and the IRR respectively as shown below.

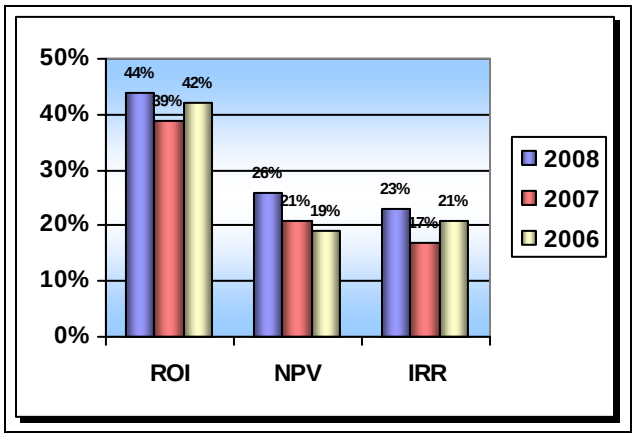


Figure 16: Percentage using the ROI, NPV and IRR

CHAPTER 4: FRAMEWORK OF RETURN ON INFORMATION SECURITY INVESTMENT

In this chapter, the major elements from information security required for the quantitative cost-benefit analysis are described together with their detailed information for each of them. Moreover a model presenting relationship between IT-security incidents and their impacts is presented.

The major inputs for the quantitative cost-benefit analysis are benefits from an information security system and costs of having the system. Figure 17 illustrates the relationship between benefits and costs.

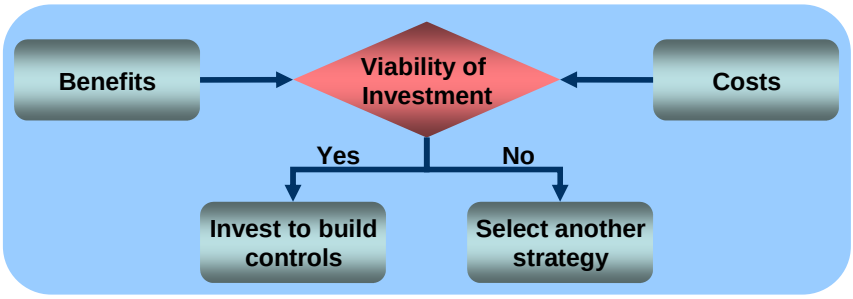


Figure 17: The overview of a cost-benefit analysis

First the benefits is explained, and then followed by the costs.

4.1 BENEFITS OF INFORMATION SECURITY INVESTMENT

As explained in this paper earlier that the benefit can be calculated from the difference between the ALE without security investment and the ALE with security investment. The ALE is taken from the SLE, which is the "total" amount of possible monetary loss from an occurrence of a risk. In 2008, Kim, Lee and In conducted a research and established a hierarchical structure of all major affecting factors by using analytic hierarchy process (AHP), resulted from IT-security incidents. The AHP is an analyzing-decision method developed by Satty (Deng and Zeng 1989). It helps to sort out multiple experts' opinions. Moreover it is very suitable when it involves high uncertainty environment with multiple evaluation criteria. The four main factors representing losses caused by IT-security incidents are lost revenue, regulatory penalties, lost productivity and reputation loss (Kim, Lee and In 2008). This result is basically derived from expert interviews, surveys, and analysis of elements.

We apply Porter's model in 1985 for firm's value chain and value system to present the business impacts from IT-security incidents in the following figure (Porter and Millar 1985).

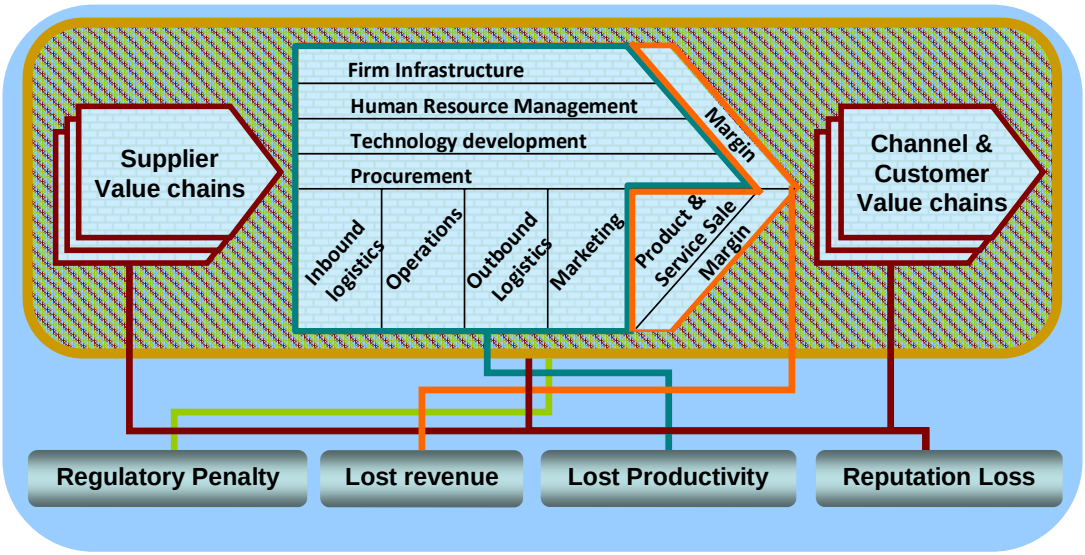


Figure 18: The business impacts caused by IT-security incidents presented with Porter's value chain and value system model

The figure shows how each factor representing losses distinguishes from each other and how its competitive advantage resulting from the difference between the ALE without security investment and the ALE with security investment covers firm's value chain and value system in its business's environment.

The whole business of a company needs to act in accordance with regulations from national and/or international institutes it involves, for instance the company must reach some certain standards specified by the government. Additionally agreements with other parties such as customers, suppliers or partners should be complied. Failure to meet these regulations or agreements generally causes monetary penalty. Therefore regulatory penalty applies to whole business environment. As a result, the main element for regulatory penalty is as follows:

- **Failure to comply with regulations or agreements** (Humaigani and Dunn 2004; Tsiakis and Stephanides 2005; Buck, Das and Hanf 2008)

More direct loss is lost revenue. It applies to the product and service sale section in the primary activity of a company and to profit margin. The first part, product and service sale, is caused by the disruption of sales and services. This basically means the company stops receiving revenue from its customers. It is one of the major problems from IT-security incidents. The second part, profit margin, is caused by damage to information assets, which cannot be fixed, or expense required recovering the company's IT system and/or information assets. Therefore the main elements for lost revenue are as follows:

- **The disruption of sale and service** (Lockstep 2004; Humaigani and Dunn 2004; ISF 2005; Tsiakis and Stephanides 2005; Neubauer, Klemen, and Biffl 2005; Buck, Das and Hanf 2008). More specifically, loss of sale can represent the disruption of sale and service.

- **Damage to information assets** (Humaigani and Dunn 2004; Buck, Das and Hanf 2008)
- **Cost of recovery** (Lockstep 2004; Humaigani and Dunn 2004; ISF 2005; Tsiakis and Stephanides 2005; Buck, Das and Hanf 2008). To recover the system after IT-security incident happens, the main elements are software, hardware and human resource for both internal employees and external consultants.

Lost productivity applies to the rest of a company's value chain for both primary activities and supporting activities. Generally when IT-security incidents are materialized, lost productivity is caused by loss of working time from both IT staff and operational staff. Lastly, IT-security incidents cause reputation loss. Stakeholders of the company can be its customers, shareholders/investors, suppliers, current/new employees, partners and other relevant communities in its business environment. When reputation is threatened, meaning that stakeholders' confidence is decreased (Buck, Das and Hanf 2008), this may result in loss of customer (Lockstep 2004; de Bie 2005; Tsiakis and Stephanides 2005; Neubauer, Klemen; and Biffl 2005) and decline in stock price (Tsiakis and Stephanides 2005).

However this thesis focuses on lost revenue and regulatory penalty, and therefore excludes lost productivity and reputation loss from the thesis scope. Figure 19 below illustrates elements for each factor representing business impacts as a result of security breach.

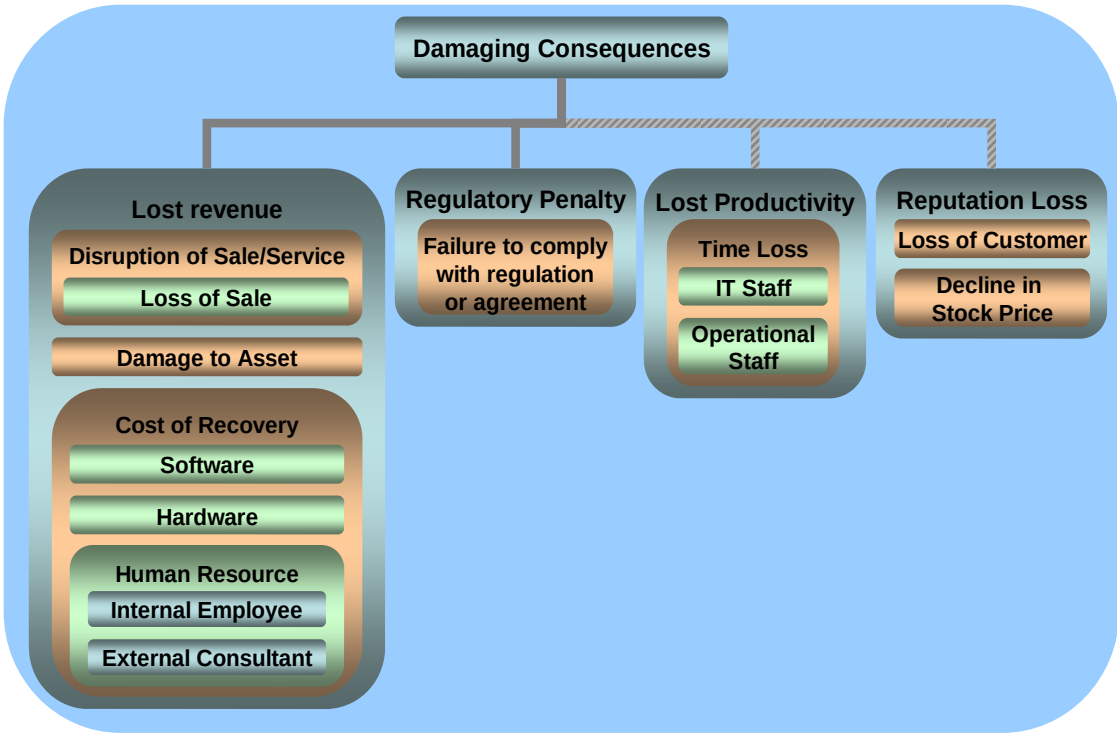


Figure 19: The business impact diagram together with sub-elements for each factor

After explaining the benefit model of information security system, the costs of the system is presented in the next section.

4.2 COSTS OF INFORMATION SECURITY INVESTMENT

The paper divides the costs of establishing and implementing information security system, or it is called *cost of control*, into two parts namely set-up cost and recurring cost. The set-up cost is expenditure that a company needs to pay to design, establish and start using an information security system. It is paid once at the beginning, while the recurring cost is annual expenditure recurred to maintain the system operating. The set-up cost consists of following costs (Lockstep 2004; Humaigani and Dunn 2004; ISF 2005):

- Software
- License fee
- Hardware
- Consultancy on analysis and configuration
- Training
- Facility

Whereas the recurring cost is basically based on two following costs (Lockstep 2004; Humaigani and Dunn 2004; ISF 2005):

- Support and maintenance fee
- Human resource for monitoring

Figure 20 below illustrates elements of the costs for both set-up and recurring costs required implement and maintain an information security system to either prevent or detect IT-security incidents.

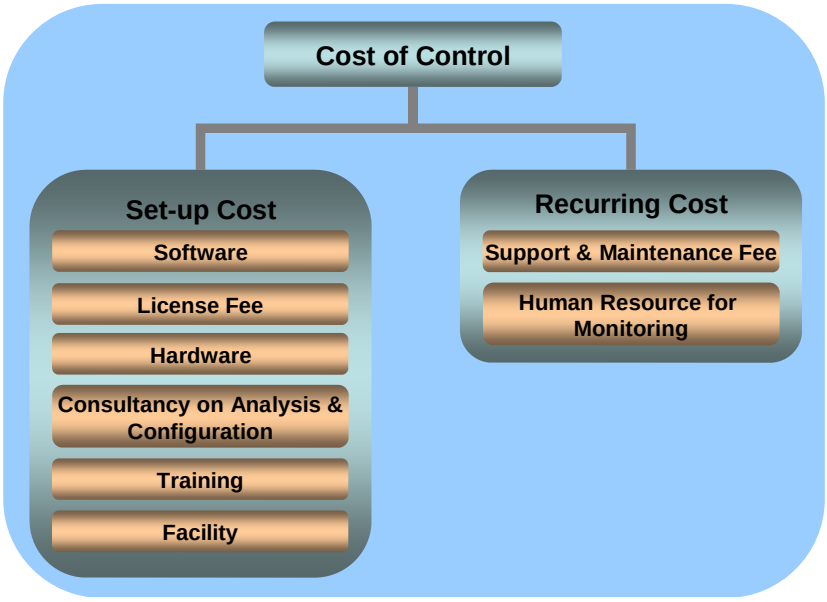


Figure 20: The cost of control diagram with subordinate costs for both set-up and recurring costs

The two previous sections explain the general benefits and costs of an information security system. The next section combines the model of the cost-benefit analysis with benefits and cost of control diagrams.

4.3 MODEL OF RETURN ON INFORMATION SECURITY INVESTMENT

We develop a model for return on information security investment based on all previous literatures, analytical judgment and results from several discussions with experts within and outside TNO. The model is presented in figure 21 below.

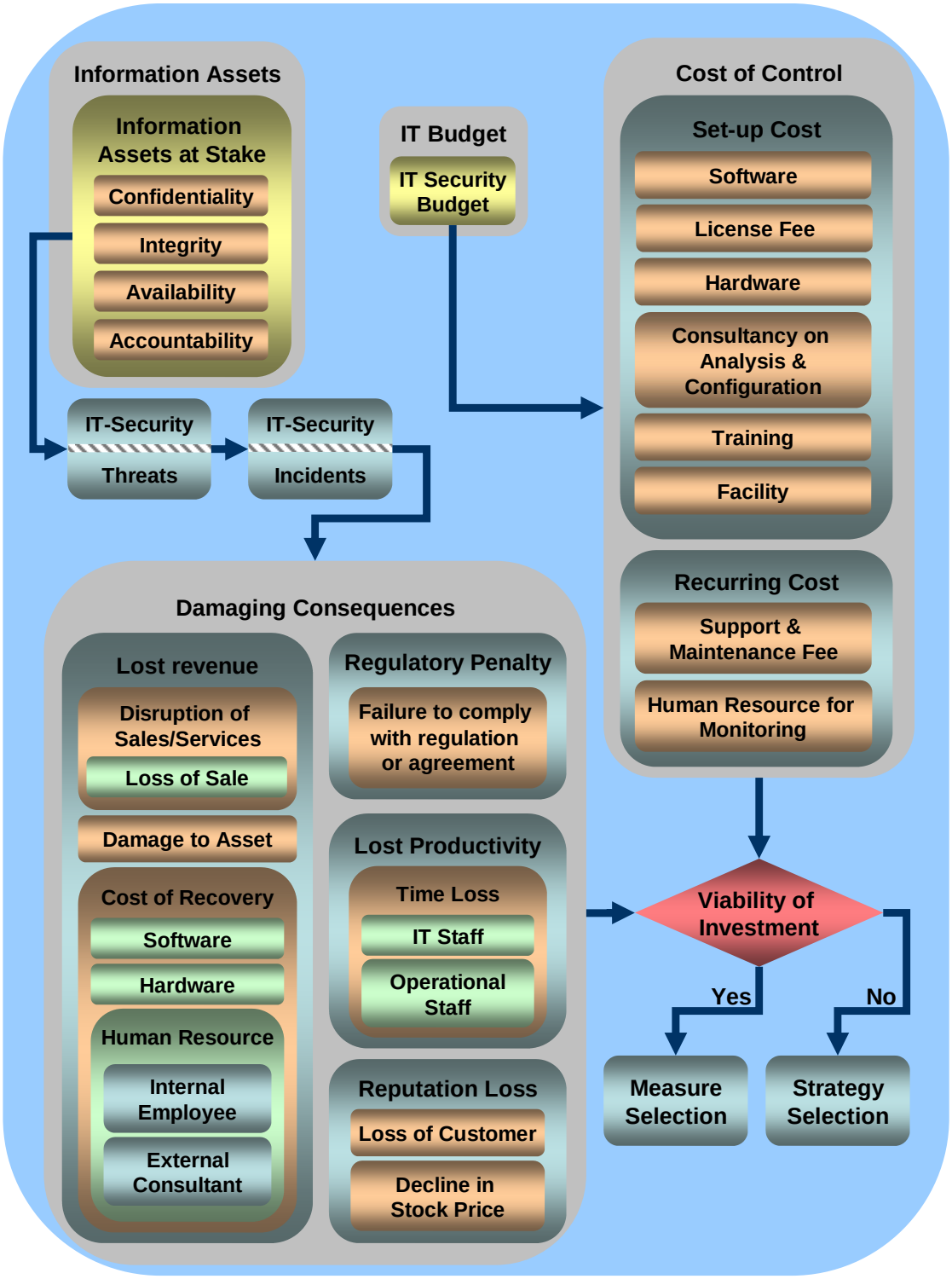


Figure 21: The model for return on information security investment

The model starts from the point that any company has information assets in its business. Some information assets are at stake, related to either one of information characteristics

namely confidentiality, integrity, availability and accountability. These assets face IT-security threats and if the threats are materialized or in the other words if the IT-security incidents happen, this will cause damaging consequences to the company. The company can select one of the strategies mentioned in chapter 3 (to recall, the strategies are acceptance, avoidance, transference and mitigation) to handle IT-security risks.

In order to prevent the IT-security incidents, the company splits IT budget for IT security purposes. If the company select the risk mitigation strategy, this IT security budget can be used for establishing and maintaining an information security system. Generally, it is viable to make an investment if benefits from the investment are more than the investment's costs. In an information security case, the company could assess an investment's benefits from the decline of damaging consequences and costs from both set-up and recurring costs. When it is viable, the company proceeds by selecting suitable countermeasures. When it is not viable, the company would rather select another strategy to cope with IT-security risks.

In this chapter, the model is developed in order to conduct the cost-benefit analysis to support assessing an information security investment. The next chapter presents an application of the ROISI model.

CHAPTER 5: APPLICATION OF RETURN ON INFORMATION SECURITY INVESTMENT

In this chapter, the application of Return on information security investment is presented and explained. Note that we use “application” and “tool” interchangeably in this chapter. To begin, general information and overview structure of the application is described. Then the explanation for each part of the tool and underlined methods of the tool are described.

5.1 GENERAL INFORMATION AND OVERVIEW STRUCTURE OF THE APPLICATION

The purpose of the application developed are to provide a structured way of capturing costs and benefits of an information security investment and to provide calculations of a number of financial returns to perform cost-benefit analysis. The financial returns applied are the ROISI, the discounted ROISI or the dROISI, the NPV and the IRR. Later, the dROISI is explained how it is developed. The balance between accuracy (therefore complexity) and simplicity is considered while the application is developed. Please note that this tool is meant to support performing a quantified risk assessment and provide numeric results from a number of financial-return methods, but not directly support selecting individual measures. It can be used to compare two or more different investments, but not compare two or more controls or countermeasures. This application should be used by users with technical knowledge and users with financial understanding to be able to generate reliable results.

This application is developed by using Microsoft Excel on Microsoft Windows XP platform and simply consists of four main parts or four Excel sheets namely the “Welcome” sheet, the “Cost of Control” sheet, the “Cost of Incident” sheet and the “Summary & Result” sheet. The structure of this application is illustrated in the figure 22 below.

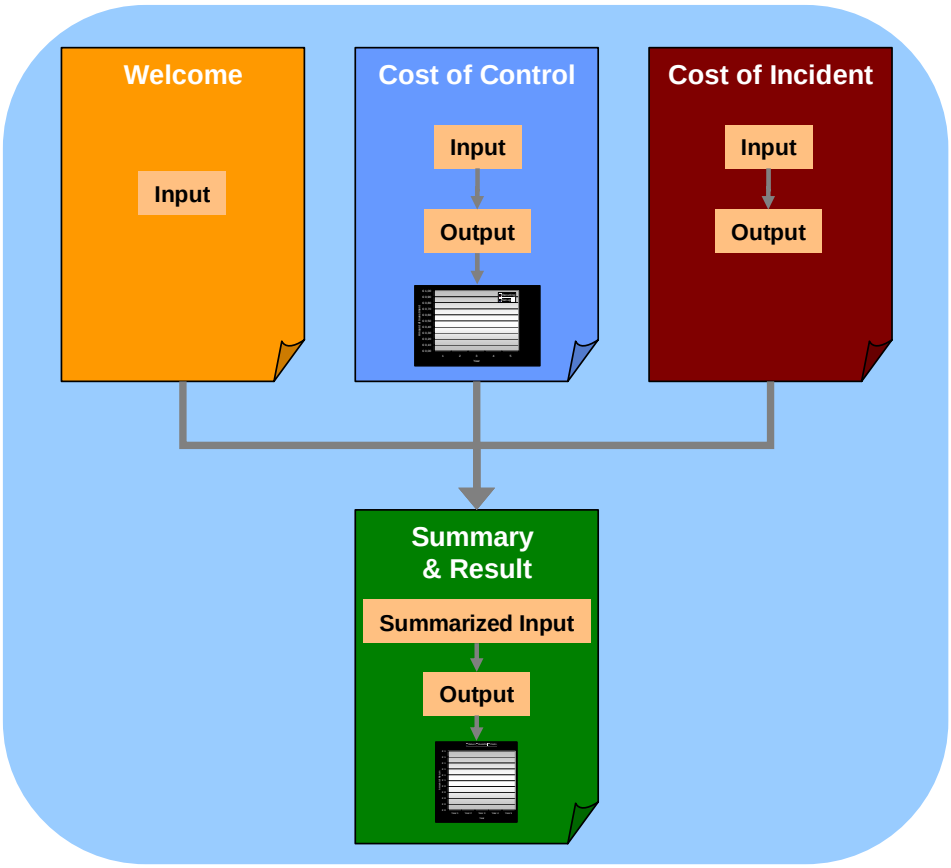


Figure 22: The overview structure of the ROISI application

First, the "Welcome" sheet explains the tool and is used to fill in general information related to the project. The "Cost of Control" sheet is used to fill in information related to controls identified together with their expected costs. The "Cost of Incident" sheet is used to assess expected impacts from IT-security risks both with and without countermeasures. The "Summary & Result" sheet summarizes all sum-up costs and benefits of the information security investment and its return in term of ROISI, dROISI, NPV and IRR.

The next section explains more detailed information about the application.

5.2 Explanation of the Application

The application identifies three different types of data in the application into three different cell colours; grey for information, blue for input from users and yellow for output calculated from the input. Users can see in the application as shown below.

	Information
	Input
	Output

Figure 23: The classification of data in the application

In the following section, each part of the tool is described.

WELCOME SHEET

The "Welcome" sheet comprises of the *introduction* part briefly explaining the purpose of the application, the *content and instruction* part briefly presenting all excel sheets in the tool and the *general information* part. The last part requires users to fill in basic information like company name, project name, analyst name, contact information for e-mail address and telephone number, date that the information security assessment is conducted, to whom the assessment is reported and the discount rate used to calculate.

The discount rate is needed in order to calculate the dROISI and the NPV for the results of the financial return. The discount rate presents a rate that decreases value of money by inflation or other factors. There are several possibilities. Some companies use a rate from Weighted Average Cost of Capital (WACC), while some use an interest rate charged by a bank. Some other companies set a 'hurdle rate', 'minimum acceptable rate of return', or 'cutoff rate', which is the minimum required rate of return on an investment a company is willing to accept before investing, given its risk and the opportunity cost of forgoing other projects (Park 2007). This rate generally is higher than the other rates. Which rate will be used depends on the culture and decision made by a company. In case that a company prefers to use WACC method for the discount rate, the company should calculate a company WACC. This company WACC is based on the company's financial capital structure. The figure below illustrates the relevant factors to compute WACC (Neuhaus 2008):

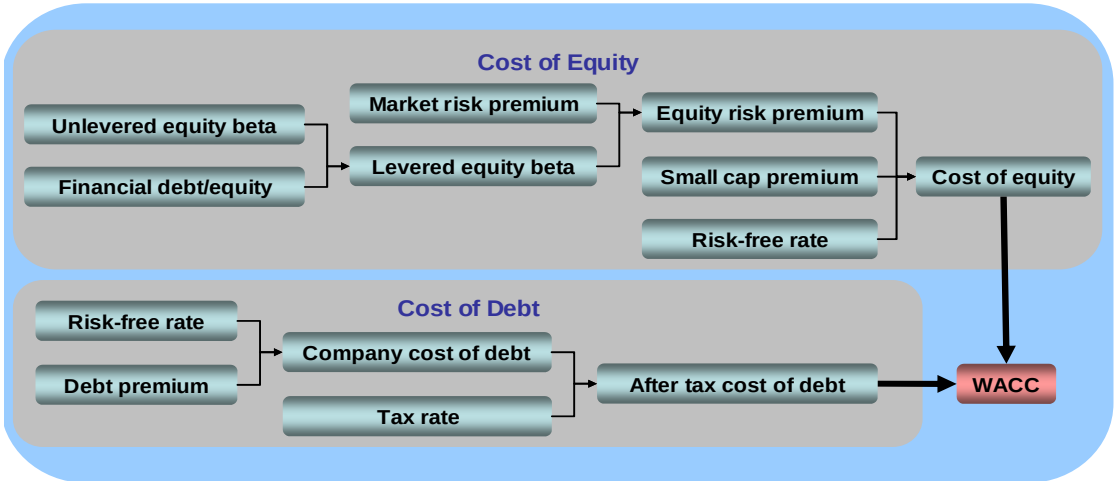


Figure 24: Approach to derive WACC for a company

Where, beta (β) measures the volatility of a security compared to the market as a whole. Unlevered equity beta (β_U) is beta with an equity ratio of 100% (or without impact of debt). Financial debt/equity is an optimal long-term capital structure. Levered beta (β_L) is unlevered beta (1 + (Debt / Equity)). Market risk premium is long-term average of the deviation of the return of risk free bonds in comparison to the return of the stock market. Small cap premium is premium for small capitalized companies, which is based on empirical studies by Ibbotson. Lastly, risk-free rate is yield of long-term government bond, normally 10-20 years. An example can be found in the appendix D.

However if the risk profile of a project differs from the risk profile of a company, the calculated company WACC needs to be adjusted.

COST OF CONTROL SHEET

The "Cost of Control" sheet mainly aims to collect information about all major costs for establishing and maintaining an information security system. In this part, users can fill in identified countermeasures together with their expected set-up costs and recurring costs. For the set-up costs, there are license fee, software, hardware, consultancy on analysis and configuration, training and facility as its main elements. For the recurring costs, there are support and maintenance fee and human resource for monitoring as its main elements. Underlined procedures in the application are presented below.

$$CC_k = \sum_{i=1}^{m} SC_{ik} + \sum_{j=1}^{n} RC_{jk}$$

where, CC_k is control cost of control *k*, which is a summation of all *m* set-up costs (*SC*) and all *n* recurring costs (*RC*). *i* represents a different type of set-up costs and *j* represents a different type of recurring costs.

$$TSC = \sum_{k=1}^{K} \sum_{i=1}^{m} SC_{ik}$$

where, *TSC* is total set-up cost from all *K* controls.

$$TRC = \sum_{k=1}^{K} \sum_{j=1}^{n} RC_{jk}$$

where, *TRC* is total recurring cost from all *K* controls.

$$TRC_t = \frac{\sum_{k=1}^{K} \sum_{j=1}^{n} RC_{jk}}{T} = \frac{TRC}{T}$$

where, TRC_t is total recurring cost from all *K* controls distributed in year *t* over a period of *T* years.

The tool takes depreciation into account, while considering total set-up costs of an investment. Depreciation is the systematic expensing of the cost of a long-lived asset that gives economic benefits more than one year (Jagels and Ralston 2006). There are four primary depreciation methods which are as follows (Friedlob and Welton 2008):

- **Straight-line depreciation method:** The method assumes that benefit is equally obtained from using an asset each year of its useful life time. The formula for straight-line depreciation method is:

$$AnnualDepreciation = \frac{Cost - SalvageValue}{UsefulLifeYears}$$

where, salvage value is an estimated value of an asset at the end of its useful life (http://www.investorwords.com/4372/salvage_value.html).

- **Units of production depreciation method:** The method assumes that benefit is obtained from the number of units of product produced by an asset. The formula for units of production depreciation method is:

$$perUnitDepreciation = \frac{Cost - SalvageValue}{UnitofProductProduced}$$

- **Sum-of-years' digits depreciation method:** The method assumes that benefit is obtained most in the early years of an asset's useful life and gradually declined in the later years. The formula for sum-of-years' digits depreciation method is:

$$yearDepreciation = \frac{(Cost - SalvageValue) * yearsInReverseOrder}{sumOfTheYear'sDigits}$$

- **Double-declining balance method:** Like sum-of-years' digits depreciation method, this method assumes that benefit is obtained most in the early years of an asset's useful life but rapidly declined in the later years with the double straight-line rate. This double straight-line rate is the most common rate used (http://en.wikipedia.org/wiki/Depreciation#Declining-Balance_Method). The formula for double-declining balance depreciation method is:

$$BookValue_0 = Cost - SalvageValue$$

$$AnnualDepreciation_t = \frac{2}{UsefulLifeYears} BookValue_{t-1}$$

$$BookValue_t = BookValue_{t-1} - AnnualDepreciation_t$$

In this application, straight-line depreciation method and double-declining balance depreciation method are used because of several reasons. The first is straight-line depreciation method is the simplest and most often used technique (http://en.wikipedia.org/wiki/Depreciation#Straight-line_depreciation). The second is declining balance depreciation method is more realistic to reflect an asset's actual expected benefit since many assets generally are more productive when they are new. The third is the double straight-line rate is the most common rate used as mentioned before. The fourth is units of production depreciation method can make the tool more complicated for users to fill in relevant information. The last is, to make use of Microsoft Excel; there is a built-in syntax especially for double-declining balance depreciation method as follows:

=DDB(cost,salvage,life,period,factor)

To apply straight-line depreciation method and double-declining balance depreciation method, salvage percentage needs to be defined in order to know the ratio of estimated scrap value at the end of assets' life and the set-up cost. Additionally, the number of years representing the number of useful life period in term of years is required as well.

As a result, the tool can calculate the set-up costs and recurring costs for each useful life year. In case of straight-line depreciation method, underlined procedure in the application is presented below.

$$TSC_t = \frac{\sum_{k=1}^{K}\sum_{i=1}^{m} SC_{ik} - \left(\sum_{k=1}^{K}\sum_{i=1}^{m} SC_{ik}\right)S}{T} = \frac{TSC - (TSC * S)}{T}$$

where, TSC_t is total set-up cost from all K controls distributed in year t over a period of T years. S is a salvage percentage. In case of double-declining balance depreciation method, underlined procedures in the application are presented below.

$$BV_0 = \sum_{k=1}^{K}\sum_{i=1}^{m} SC_{ik} - \left(\sum_{k=1}^{K}\sum_{i=1}^{m} SC_{ik}\right)S = TSC - (TSC * S)$$

$$TSC_t = \left(\frac{2}{T}\right)BV_{t-1}$$

$$BV_t = BV_{t-1} - TSC_t$$

where, BV is book value derived from total set-up cost from all K controls minus its salvage value.

$$C_t = TSC_t + TRC_t$$

where, C_t is all costs in year t. Besides from all the calculations, the "Cost of Control" sheet plots a graph for the amount of investment for both the set-up costs and the recurring costs for each year as shown in the next section.

COST OF INCIDENT SHEET

The "Cost of Incident" sheet mainly aims to collect information about likelihood and impact of any potential IT-security incident for each information asset at stake. In this part, users can first make adjustments in the frequency level table as well as in the risk-rating scale table. An example from the application for the quantification of frequency table and the risk-rating scale table is presented below in table 5 and 6. According to expert interviews, this depends on each project situation and intention. In some cases, after the users make adjustments, they should not make new adjustment in these two tables again. This is to prevent any party to adjust the risk level to match their own preference. However, in some other cases, it may be more beneficial for both parties to adapt the risk-rating scale table again in order to present better information.

Table 5: The quantification of frequency from the application

Frequency level	Description	Quantified freq.
Negligible	Unlikely to occur	0,05
Very Low	Likely to occur 2-3 times every 5 years	0,5
Low	Likely to occur once every year or less	1,0
Medium	Likely to occur once every 6 months or less	2,0
High	Likely to occur once per month or less	12,0
Very High	Likely to occur multiple times per month or less	50,0
Extreme	Likely to occur multiple times per day	500,0

Table 6: The risk-rating scale from the application

Risk scale				Risk level
0	-	10.000		Negligible
10.001	-	50.000		Low
50.001	-	200.000		Medium
200.001	-	1.000.000		High
1.000.001	-	10.000.000		Critical

After first setting these two tables, users can identify potential IT-security incidents together with their effects. Then experts can select the frequency level or indicate the ARO themselves for situations with and without controls. For example users identify "unauthorized physical access to core infrastructure components" as one of potential IT-security incidents. Its effect is the elimination of components as a result of which the service is not available. The frequency level of this incident without control is "Medium", meaning that it may happen once in six months; however, it can be reduced to "Low" with control(s). Next, users fill in numeric values for the impact of the incident's single occurrence as well for both with and without controls. According to the model developed, this consists of loss of sale, damage to asset, cost of recovery (cost for software, hardware, internal employee and external consultant), regulatory penalty and others. At the "others" column, users can make an adjustment to some other important elements based on specific cases for instance loss of life in hospital. Note that this is only an example and we do not intend to bring up the ethic issue here.

As discussed with several TNO experts, the total impact of an incident with control is equal to the total impact of an incident without controls in many cases. This is because many controls decrease the likelihood of an incident rather than decrease its impact. The tool aids users by providing information in a drop-down list, while the users can give another numeric value when the impact can be reduced.

Then the tool computes all assets' benefits of the investment. With a use of Microsoft Excel, the ARO is quantified by using a built-in syntax to match frequency level with its numeric value as shown below.

=VLOOKUP(lookup_value,table_array,col_index_num,range_lookup)

For a without control situation, underlined procedures in the application are presented below.

$$SLE_q = \sum_{p=1}^{a} I_{pq}$$

where, SLE_q is single loss exposure of potential IT-security incident q, which is a summation of it's a impacts. p represents a different type of impacts.

$$ALE_q = ARO_q * SLE_q$$

where, ALE_q is annual loss expectancy of a potential IT-security incident q, which is a multiplication of ARO_q (annual rate of occurrence) and SLE_q of the incident q.

Similarly to the without control situation, for a with control situation, underlined procedures in the application are presented below.

$$rSLE_q = \sum_{p=1}^{a} rI_{pq}$$

where, $rSLE_q$ is residual single loss exposure of potential IT-security incident q, which is a summation of its residual impacts. p represents a different type of impacts.

$$rALE_q = rARO_q * rSLE_q$$

where, $rALE_q$ is residual annual loss expectancy of a potential IT-security incident q, which is a multiplication of $rARO_q$ (residual annual rate of occurrence) and $rSLE_q$ of the incident q.

$$B_q = ALE_q - rALE_q$$

where, B_q is benefit obtained from the difference of annual loss expectancy with and without controls of the incident q.

$$TB_a = \sum_{q=1}^{Q} B_{qa}$$

where, TB_a is total benefit from asset a.

$$TB_t = \sum_{a=1}^{A} \sum_{q=1}^{Q} B_{qa} = \sum_{a=1}^{A} TB_a$$

where, TB_t is total benefit from all assets from the investment in one year.

SUMMARY AND RESULT SHEET

The "Summary and Result" sheet mainly aims to provide summarized information about all costs and benefits of an information security investment. More importantly, this sheet presents the investment's financial returns in four different methods namely ROISI, dROISI, NPV and IRR. As presented in chapter 3 about ROISI, NPV and IRR, we decide to consistently use all methods mentioned because these three methods are generally used. When decision makers compare any information security investment with other kinds of business investments or even another information security investment, there will not be a problem of consistency.

Additionally, the dROISI is developed since the ROI is the most popular approach as mentioned earlier; however, the weakest point of this approach is that it does not take into account time value of money. The discount ROI or dROI is first developed by applying the basic concept of the ROI and NPV. For usage of information security assessment, the dROISI is developed by combining the concept of the dROI and ROISI together. The dROISI directly strengthens this point. Instead of the ROISI approach as shown below, applied from the ROI, the dROI and the dROISI use the present value of all benefits and costs generated in different years as shown below.

$$ROISI = \frac{ALE_{withoutsafeguards} - ALE_{withsafeguards} - Cost_{safeguards}}{Cost_{safeguards}}$$

$$dROI = \frac{\sum_{t=0}^{T} \frac{Benefit_t}{(1+r)^t} - \sum_{t=0}^{T} \frac{Cost_t}{(1+r)^t}}{\sum_{t=0}^{T} \frac{Cost_t}{(1+r)^t}} = \frac{Benefit_{NPV} - Cost_{NPV}}{Cost_{NPV}}$$

$$dROISI = \frac{\sum_{t=0}^{T} \frac{ALE_{t(withoutsafeguards)} - ALE_{t(withsafeguards)}}{(1+r)^t} - \sum_{t=0}^{T} \frac{Cost_{t(safeguards)}}{(1+r)^t}}{\sum_{t=0}^{T} \frac{Cost_{t(safeguards)}}{(1+r)^t}}$$

The table 7 compares the four approaches presented earlier in chapter 3 and in this chapter.

Table 7: The comparison for all approaches

Approach	ROI/ROISI	dROI/dROISI	NPV	IRR
Magnitude	No	No	Yes	No
Time value of money	No	Yes	Yes	Yes
Complexity	Low	Medium/High	High	High
Popularity	High	-	Medium	Medium/Low
Comment	Less reliable than the other two approaches	More reliable than the ROISI approach	Sensitive to the time value of money which has limited information	doubtful assumption: the whole period has the same rate of return

Then the tool computes the financial returns of an investment with all summarized information about all costs and benefits. In the summary table, underlined procedures in the application are presented below.

$$C_t = TSC_t + TRC_t$$

From the "Cost of Control" sheet, the application computes the total set-up cost, total recurring cost and total cost for each year.

$$TSC = \sum_{t=0}^{T} TSC_t$$

where, *TSC* is total set-up cost from every year.

$$TRC = \sum_{t=0}^{T} TRC_t$$

where, *TRC* is total recurring cost from every year.

$$C = \sum_{t=0}^{T} C_t = \sum_{t=0}^{T} TSC_t + \sum_{t=0}^{T} TRC_t$$

where, *C* is total costs from every year.

$$TB_t = \sum_{a=1}^{A} \sum_{q=1}^{Q} B_{qa} = \sum_{a=1}^{A} TB_a$$

From the "Cost of Incident" sheet, the application computes the total benefit for each year.

$$TB = \sum_{t=0}^{T} TB_t$$

where, *TB* is total benefits from every year.

$$R_t = TB_t - C_t$$

where, R_t is return of the investment, which is the difference between total benefit and total cost for each year.

$$R = \sum_{t=0}^{T} R_t = \sum_{t=0}^{T} TB_t - \sum_{t=0}^{T} C_t$$

where, *R* is total return of the investment for every year.

In the financial return result table, underlined procedures in the application are presented below.

$$ROISI = \frac{\sum_{t=0}^{T} TB_t - \sum_{t=0}^{T} C_t}{\sum_{t=0}^{T} C_t} = \frac{TB - C}{C} = \frac{R}{C}$$

$$dROISI = \frac{\sum_{t=0}^{T} \frac{TB_t}{(1+r)^t} - \sum_{t=0}^{T} \frac{C_t}{(1+r)^t}}{\sum_{t=0}^{T} \frac{C_t}{(1+r)^t}} = \frac{TB_{NPV} - C_{NPV}}{C_{NPV}} = \frac{R_{NPV}}{C_{NPV}}$$

$$NPV = \sum_{t=0}^{T} \frac{TB_t - C_t}{(1+r)^t}$$

In the Microsoft Excel, there is a built-in syntax for the NPV method as follows.

=NPV(rate,value1,value2, ...)

$$NPV = \sum_{t=0}^{T} \frac{TB_t - C_t}{(1+IRR)^t} = 0$$

In the Microsoft Excel, there is a built-in syntax for the IRR method as follows.

=IRR(values,guess)

Besides from all the calculations, the "Summary and Result" sheet plots a graph for the return, cost and benefit of the investment for each year as shown in the next section.

5.3 THE APPLICATION'S EXAMPLE

In this section, an example using the application is presented. Please note that the example is totally not derived from any sources.

THE "WELCOME" SHEET

Table 8: The example for general information

General Information		
Company name		The company A
Project name		RACIF (Risk Assessment - Core Infrastructure)
Analyst		Mai Panchit Puangsri
Contact information		
Email		p.puangsri@student.tudelft.nl
Telephone		0031616682649
Date		17 June 2009
Discount rate		5,00%
Reported to		Jan van den Berg and Femke Hulsbergen

THE "COST OF CONTROL" SHEET

Table 9: The example for investment distribution information

Depreciation Method		Double-declining-balance method
No. of years		5
Salvage percentage		5%

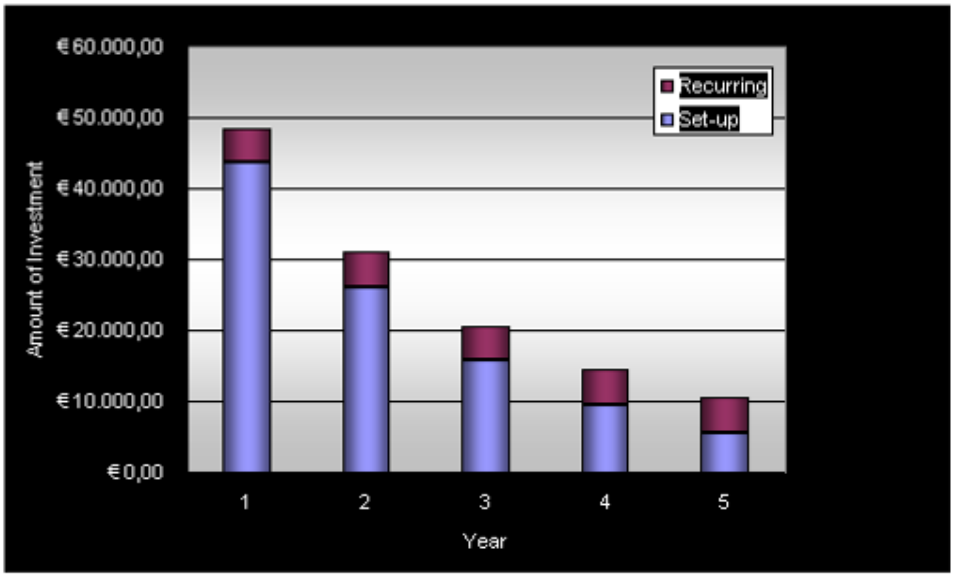
Table 10: The example of control information for both set-up cost and recurring cost

Control		Set-up cost							Recurring cost			
Control name	ID	License fee	Software	Hardware	Consultancy on analysis &	Training	Facility	Total	Support & maintenance fee	Human resource for monitoring	Total	Total
Control name A	M1	€500	€4.000	€0	€2.000	€0	€0	€6.500	€1.000	€2.000	€3.000	€7.100
Control name B	M2	€1.000	€3.000	€500	€2.000	€0	€500	€7.000	€500	€1.500	€2.000	€7.400
Control name C	M3	€2.500	€5.000	€0	€4.500	€0	€0	€12.000	€500	€4.000	€4.500	€12.900
Control name D	M4	€0	€2.000	€5.000	€1.000	€0	€0	€8.000	€500	€1.200	€1.700	€8.340
Control name E	M5	€3.000	€1.000	€0	€1.000	€0	€0	€5.000	€1.000	€2.000	€3.000	€5.600
Control name F	M6	€0	€10.000	€2.000	€5.000	€500	€500	€18.000	€1.000	€1.000	€2.000	€18.400
Control name G	M7	€0	€7.500	€500	€1.000	€3.500	€100	€12.600	€500	€1.000	€1.500	€12.900
Control name H	M7	€0	€3.000	€500	€2.000	€0	€100	€5.600	€500	€500	€1.000	€5.800
Control name I	M8	€2.000	€1.000	€1.000	€1.000	€0	€100	€5.100	€1.000	€1.000	€2.000	€5.500
Control name J	M9	€0	€2.000	€2.000	€2.500	€1.000	€500	€8.000	€1.000	€1.500	€2.500	€8.500
Control name K	M10	€1.000	€1.000	€10.000	€4.000	€5.000	€100	€21.100	€500	€1.000	€1.500	€21.400
Total		€10.000	€39.500	€21.500	€26.000	€10.000	€1.900	€108.900	€8.000	€16.700	€24.700	€113.840

Table 11: The example for summarized information

	Year 1	Year 2	Year 3	Year 4	Year 5
Set-up	€ 43.560,00	€ 26.136,00	€ 15.681,60	€ 9.408,96	€ 5.645,38
Recurring	€ 4.940	€ 4.940	€ 4.940	€ 4.940	€ 4.940
Annual sum	€ 48.500,00	€ 31.076,00	€ 20.621,60	€ 14.348,96	€ 10.585,38

Table 12: The example for the "investment in each year" graph



THE "COST OF INCIDENT" SHEET

Table 13: The example of frequency quantification

Frequency level	Description	Quantified freq.
Negligible	Unlikely to occur	0,05
Very Low	Likely to occur 2-3 times every 5 years	0,5
Low	Likely to occur once every year or less	1,0
Medium	Likely to occur once every 6 months or less	2,0
High	Likely to occur once per month or less	12,0
Very High	Likely to occur multiple times per month or less	50,0
Extreme	Likely to occur multiple times per day	500,0

Table 14: the example of the risk-rating scale

Risk scale				Risk level
0	-	10.000		Negligible
10.001	-	50.000		Low
50.001	-	200.000		Medium
200.001	-	1.000.000		High
1.000.001	-	10.000.000		Critical

Table 15: The example of incidents' information without controls

Asset:	Asset A	Asset ID:	A1		Without controls									
Security aspect	ID	Potential IT-security incident	Description of the incident's effects	Likelihood (ARO)	Impact (SLE)								Total impact (SLE)	Risk (ALE)
					Loss of sale	Damage to asset	Cost of recovery				Regulatory penalty	Others		
							Software	Hardware	Internal employee	External consultant				
Confidentiality	A1 C1	Incident A	Effect A	Low	0	5.000	500	0	0	0	20.000	0	25.500	25.500
	A1 C2	Incident B	Effect B	Medium	0	10.000	1.000	0	0	0	0	0	11.000	22.000
	A1 C3	Incident C	Effect CA Effect CB	1,5	0	5.000	500	500	0	0	10.000	0	16.000	24.000
Integrity	A1 I1	Incident D	Effect D	Low	0	1.000	500	0	3.000	0	0	0	4.500	4.500
	A1 I2	Incident E	Effect E	Very High	5.000	500	500	0	0	0	0	0	6.000	300.000
	A1 I3	Incident F	Effect F	Medium	0	500	2.000	0	0	0	0	0	2.500	5.000
Availability	A1 A1	Incident G	Effect GA Effect GB Effect GC	High	10.000	0	500	0	2.000	0	5.000	0	17.500	210.000
	A1 A2	Incident H	Effect H	Low	4.000	0	1.000	2.000	2.500	1.000	0	0	10.500	10.500
	A1 A3	Incident I	Effect I	Medium	3.000	0	500	0	3.000	0	1.000	0	7.500	15.000
Total					22.000	22.000	7.000	2.500	10.500	1.000	36.000	0	101.000	616.500

Asset:	Asset B	Asset ID:	A2		Without controls									
Security aspect	ID	Potential IT-security incident	Description of the incident's effects	Likelihood (ARO)	Impact (SLE)								Total impact (SLE)	Risk (ALE)
					Loss of sale	Damage to asset	Cost of recovery				Regulatory penalty	Others		
							Software	Hardware	Internal employee	External consultant				
Confidentiality	A2 C1	Incident A	Effect A	Very High	0	2.500	500	0	0	0	2.000	0	5.000	250.000
	A2 C2	Incident C	Effect C	Low	1.000	8.000	1.000	0	2.000	1.000	10.000	0	23.000	23.000
Integrity	A2 I1	Incident D	Effect DA Effect DB	Low	0	1.000	500	0	3.000	1.000	0	0	5.500	5.500
	A2 I2	Incident E	Effect E	1,5	0	2.000	500	500	0	0	5.000	0	8.000	12.000
	A2 I3	Incident F	Effect F	Low	0	5.000	500	0	0	0	20.000	0	25.500	25.500
Availability	A2 A1	Incident G	Effect G	Very Low	2.500	10.000	1.000	0	0	500	0	0	14.000	7.000
	A2 A2	Incident I	Effect IA Effect IB Effect IC	High	1.000	0	600	0	1.000	0	0	0	2.600	31.200
Total					4.500	28.500	4.600	500	6.000	2.500	37.000	0	83.600	354.200

Asset 1		22.000	22.000	7.000	2.500	10.500	1.000	36.000	0	101.000	616.500
Asset 2		4.500	28.500	4.600	500	6.000	2.500	37.000	0	83.600	354.200
Total		26.500	50.500	11.600	3.000	16.500	3.500	73.000	0	184.600	970.700

Table 16: The example of incidents' information with controls

With controls													
Control	Residual likelihood (rARO)	Residual impact (rSLE)								Total residual impact (SLE)	Residual risk (rALE)	Comment	ΔALE = (ALE-rALE)
		Loss of sale	Damage to asset	Cost of recovery				Regulatory penalty	Others				
				Software	Hardware	Internal employee	External consultant						
M2, M5, M7	0,8	0	5.000	500	0	0	0	20.000	0	25.500	20.400		5.100
M4	Low	0	8.000	1.000	0	0	0	0	0	9.000	9.000		13.000
M2, M8	Low	0	5.000	500	500	0	0	10.000	0	16.000	16.000		8.000
M1, M3, M4	Negligible	0	1.000	500	0	3.000	0	0	0	4.500	225		4.275
M7	Very High	4.800	500	500	0	0	0	0	0	5.800	290.000		10.000
M2, M3, M9	Low	0	500	2.000	0	0	0	0	0	2.500	2.500		2.500
M5, M10	High	8.500	0	500	0	2.000	0	5.000	0	16.000	192.000		18.000
M10	Very Low	4.000	0	1.000	2.000	2.500	1.000	0	0	10.500	5.250		5.250
M7, M9	1,5	3.000	0	500	0	3.000	0	1.000	0	7.500	11.250		3.750
		20.300	20.000	7.000	2.500	10.500	1.000	36.000	0	97.300	546.625		69.875

With controls													
Control	Residual likelihood (rARO)	Residual impact (rSLE)								Total residual impact (SLE)	Residual risk (rALE)	Comment	ΔALE = (ALE-rALE)
		Loss of sale	Damage to asset	Cost of recovery				Regulatory penalty	Others				
				Software	Hardware	Internal employee	External consultant						
M2, M6, M7, M9	45	0	2.500	500	0	0	0	2.000	0	5.000	225.000		25.000
M6, M8, M10	Low	1.000	5.000	1.000	0	2.000	0	10.000	0	19.000	19.000		4.000
M1, M3, M4	Very Low	0	1.000	500	0	3.000	1.000	0	0	5.500	2.750		2.750
M6, M9	Low	0	2.000	200	500	0	0	5.000	0	7.700	7.700		4.300
M3	Low	0	4.000	500	0	0	0	20.000	0	24.500	24.500		1.000
M5, M9, M10	Negligible	2.500	10.000	500	0	0	500	0	0	13.500	675		6.325
M2, M6, M7, M9	10	1.000	0	500	0	1.000	0	0	0	2.500	25.000		6.200
		4.500	24.500	3.700	500	6.000	1.500	37.000	0	77.700	304.625		49.575

	20.300	20.000	7.000	2.500	10.500	1.000	36.000	0	97.300	546.625	69.875
	4.500	24.500	3.700	500	6.000	1.500	37.000	0	77.700	304.625	49.575
	24.800	44.500	10.700	3.000	16.500	2.500	73.000	0	175.000	851.250	119.450

THE "SUMMARY AND RESULT" SHEET

Table 17: The example for summarized input table

Summary						
	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Benefits	€119.450	€119.450	€119.450	€119.450	€119.450	€597.250
Costs	€48.500	€31.076	€20.622	€14.349	€10.585	€125.132
Set-up cost	€43.560	€26.136	€15.682	€9.409	€5.645	€100.432
Recurring cost	€4.940	€4.940	€4.940	€4.940	€4.940	€24.700
Return	€70.950	€88.374	€98.828	€105.101	€108.865	€472.118
Depreciation method	Double-declining-balance method					
Discounted factor	5,00%					

Table 18: The example for the "return-benefit-cost in each year" graph

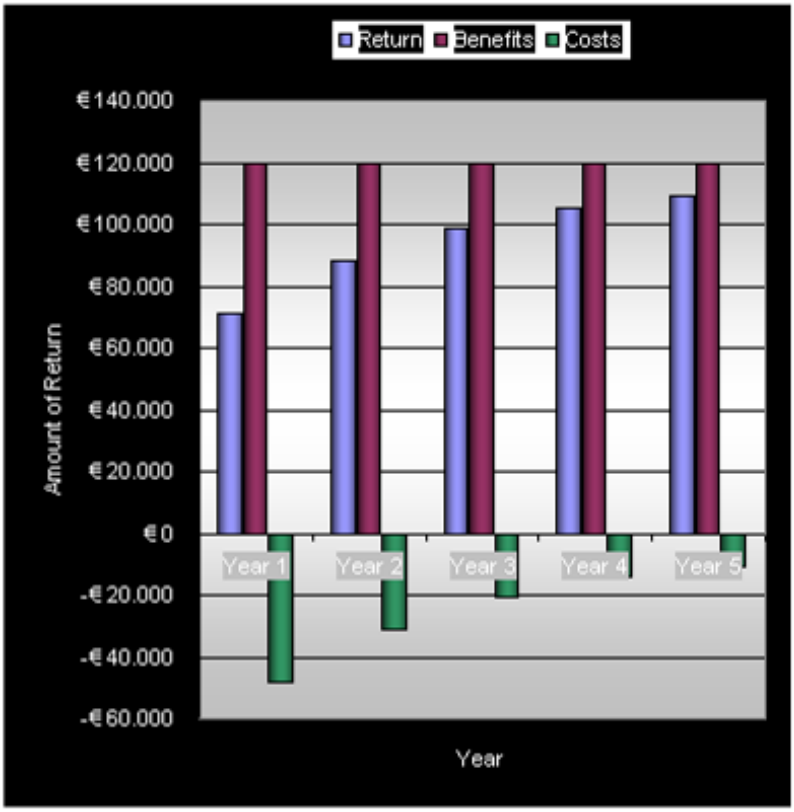


Table 19: The example for financial return result

Financial return	Result	Comment
ROISI	377,3%	
dROISI	360,6%	
NPV	€404.866	
IRR	107,8%	

CHAPTER 6: EVALUATION OF THE MODELS AND THE APPLICATION

To clarify, evaluation in this research generally refers to a process of checking that the models and the application meet specifications and that they fulfil its intended purpose. In this chapter, the process used to evaluate the models and tool is described together with its detailed approach. Then the results from the evaluation are presented. At the end the analysis from all interviews' results and from observing during the meetings is presented as well.

6.1 APPROACH

In order to evaluate the models and the application developed, we would initially like to apply case study research design because it is particularly functional to test theoretical models by applying them in several real cases. Generally case study is an intensive study of one or a few cases, meaning that it is rather specific to the study cases. On the other hand, case study provides a more realistic view. However conducting case study is impossible due to several reasons. One reason is resources availability, especially time, are limited. Another reason is information needed to be collected for the application is highly sensitive since it is closely related to its reputation. Please note here that the evaluation part is conducted under time limitation. As a consequence, we are aware that the evaluation may not perfectly verify the models and the application, but rather give insight on some essential relevant topics from empirical information.

"*Interview*" is used to gather information because of several reasons. First, even though the models and tool are generically developed, using qualitative approach can support to recognize individuality of different situations in which the models and tool are possibly applied. Second, comparing with other gathering methods like questionnaire, observation and archival data, interview gives analysts more control and makes complex issues possible to be collected. Especially when assessing the models and tool for quantified return on information security investment, this involves many different issues altogether. However we realize that first this method is resource intensive and second the interviewer (the researcher) may have influence on the results. The first issue is taken care by planning and scheduling the interview meeting early enough, for instance the interviewer can conduct two interviews in Groningen on the same day. The second issue is prevented by forming questions carefully and avoiding all kinds of leading questions.

At the very beginning of the research, unstructured interview is applied because it is useful to explore the topic. To evaluate the models and tool, semi-structured interview is applied because of several reasons. For instance, with well-structured but open-ended questions, this can prevent missing some important topics, while giving room for flexibility to adjust the

interviews based on individual interviewee's different experiences. However the major disadvantage of the semi-structured interview is its limitation of generalization.

The selection of interviewees is employed both snowball sampling and convenience sampling strategies. The snowball sampling strategy is when the interviewees are picked because they are the key persons. On the other hand, the convenience sampling strategy is when the interviewees are selected because of convenience reason. We cannot confirm that the interviewees are the best representatives of the whole population; therefore, due to the convenience reason, they were picked since they are ones of the most suitable experts reachable for the interviews.

Some information about the interviewees is as follows:

- The interviewees are working at TNO ICT in the security department in different positions namely: senior security consultant, innovator/consultant and project employee.
- They have been working on qualitative risk assessment and/or qualitative assessment of information security investment in several projects for a number of companies.
- They will most likely be the ones who are going to use the application afterwards.

After the interviewees were selected, we distributed the models and the application to three key experts about a week and a half in prior to the appointed interview date and asked them to investigate the application. It was followed by an individual semi-structured interview. Several open-ended questions were posed. The structure of the interviews is illustrated in figure 25.

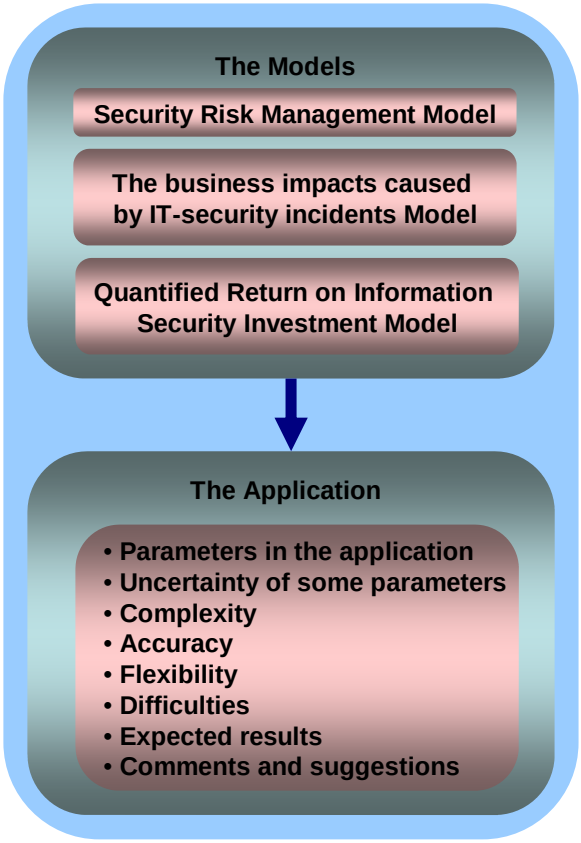


Figure 25: The interview structure

According to the approach described earlier, the two common quality criteria generally are reliability and validity.

- **Reliability:** In order to ensure reliability, *transparency* in this section is relatively acceptable since the report explains not only results but also the approach we employed.
- **Validity:** At the very beginning of the research, applying *face validity*, we discussed with a few experts whether the approach seems to be reasonable or not. Due to the fact that experts are human which may forget or make errors, the interviews were conducted with three experts. This may help to reduce possible human mistakes.

In the next section, results from the three interviews are described.

6.2 Summarized Results from The Interviews

First Interview

According to the interview, the models are rather practical and clear. The interviewee mentioned that in some cases, TNO ICT has a pre-defined milestone and gates before proceeding to the next ones. For instance, the company A asks TNO ICT to conduct a

Business Impact Assessment (BIA) and then it may be followed by a quick risk assessment of the company A's existing information security system. At this stage there is no control identification and/or control analysis. Lastly, the company A may ask TNO ICT to conduct a detailed risk assessment. The application is beneficial and suitable for the quantified detailed risk assessment since it assists experts to conduct the analysis to be more accurate. On the other hand, the complexity of the application may be high when users apply the application to the quick risk assessment. Some comments are that the application does not directly support decision makers to select a specific countermeasure. However the application does satisfy the need of assessing return of an information security investment and makes it possible to compare among different investments. Some suggestions are that it may be necessary to freeze the risk-rating scale table after a discussion at the beginning between analysts and the client company to avoid any influenced adjustment and therefore to ensure accountability of the analysis. Another suggestion is that it can be necessary to add a "Comment" column in the "Cost of Control" sheet in order to clarify several relevant issues. For instance, users can indicate there how many software users are for the specified cost of license fee.

SECOND INTERVIEW

According to the interview, the models are rather good and complete. The application is very usable and high-quality. However, for complexity, it indeed depends on the project scope from a client company and the level that TNO ICT needs to investigate. Once TNO ICT needs to investigate the detailed risk assessment, the tool will be very helpful for analysts and it is not too complex. The application yields flexibility for different cases because it gives rooms for adjustment according to a case's requirements. Additionally in slightly contrast with the first interview; he mentioned that the application is not too complex. This is because, for instance, experts do not need to fill all parameters of an IT-security incident's impact. However the application does remind experts to think about all important elements. When some elements have insignificant financial impact, they can leave those parameters blank. Some suggestions are that it may be more beneficial if the word "IT" changes to "Information" in the models and the application so that the models and the application can have broader scope, which they are applicable as well. With drop-down lists in the part of "with controls" in the application, the application helps and makes users fill in information at the part of "with controls" faster because in many cases controls reduce only likelihood (not impact) of IT-security incident. In order to support the quick risk assessment, the application needs some adjustment in order to simplify the application as the need from the quick risk assessment. At the "Summary and Result" sheet, the summarized information can include the set-up cost information as well. When discussing about uncertainty, the interviewee cited that it is rather difficult to get or estimate information about the distribution of input information. At the end, the interviewee reminded us that the set-up cost can be referred as CAPEX (Capital Expenditure), while the recurring cost can be referred as OPEX (Operational Expenditure). These two terms would be more recognizable by business oriented users.

THIRD INTERVIEW

According to the interview, the model is sensible due to practical experiences. When investigating the uncertainty part in the model, the uncertainty should indeed be present in the Risk management model. However the major reason that it is not yet be present in many standards is that it will consume a lot of resources to conduct uncertainty assessment. Another reason is that in some cases, there is very high uncertainty. This may cause results from the analysis become meaningless from the interviewee's point of view. When interviewing about the application, the interviewee stated that this tool should definitely be one of tools that TNO should have. It is helpful in generic sense; however, it may need an adjustment to fit well to some really specific cases. Overall, the presentation of the application is very nice. This needs to be taken care of because the application should not be used by only business people but also more towards technical ones. Some suggestions are that when the application is further developed, it could be wise to separate the parts filled by business people and by technical ones. When considering impacts of IT-security incidents, the "internal employee" element of the "cost of recovery" may be rather hard to quantify compared with the other elements. Another suggestion is that the "Welcome" sheet should probably include project scope in order to make it clarify what will be assessed and what will not.

In the next section, the results of the three interviews are analysed and presented.

6.3 ANALYSIS OF THE RESULTS FROM THE INTERVIEWS

In this section, the analysis of the results is presented. The analysis is taken from the results of the interviews together with observation during the meetings.

From the three interviews, we can sum up that the models are rather practical, good, clear and useful. When discussing about the models, the interviewees agree upon the models. For the security risk management model, most interviewees have a concern at the part related to the way how to select a strategy coping with risks; however, this is out of scope of the thesis. We should have informed the scope of the research since the beginning. The uncertainty assessment part in the model is new but somewhat crucial and beneficial. This part can be hard and time-consuming when implementing it.

When discussing about the application of the ROISI model, the application gets very positive feedbacks from the interviewees, especially when users apply it to conduct the detailed risk assessment analysis. The parameters in the application are generic but they will need an adjustment to some specific cases in order to better fit in different situations. The complexity is not high when the application is employed for the detailed risk assessment. For the quick risk assessment, the application can be considered too complex. Despite the fact that the application has never been tested with real cases, the interviewees believe that this application yields high accuracy for the results of the analysis. According to the interviewees' knowledge and experiences, it can be concluded that the flexibility of the application is high. This could be the key that makes the application applicable to other cases. The difficulty of the application itself is relatively low. The application is easy to use and fairly user-friendly.

However the difficulty to eventually complete the analysis using this application mainly comes from a few sources. One is finance knowledge of analysts; it seems like the analysts may have a small difficulty in understanding the financial terms for instance discount rate, depreciation methods, ROISI, dROISI, NPV and IRR. The other is lack of information about the likelihood and the impact of IT-security incidents. However with the use of drop-down lists at the likelihood and at the "without control" part and with the sub-elements of impact, the application can overcome some difficulties. The sub-elements of impact can assist experts to think about all relevant important issues. Smaller estimations can support experts to estimate and make the estimations easier than the one big whole estimation. It can be summed up from the interviews that the results presented in the application are rather complete and satisfy the current needs. Especially the presentations of the summarized information and the results are pretty nice. However several practical suggestions are received. For instance the project scope and the summarized set-up costs can be added to the application.

Please note here that even though the models and the application are developed based on the findings from literature, we have been working at TNO ICT, discuss several issues with experts from TNO ICT, investigate the way how TNO ICT conducts qualitative risk assessment and conduct the interviews with experts from TNO ICT. As a result, the generalization of the research results may possibly be influenced.

In this chapter, the evaluation of the models and application is presented. This includes its approach, results and analysis of the results. The next and last chapter describes the overall findings which answer the research questions. Lastly, recommendation for further research for any researchers is presented.

CHAPTER 7: CONCLUSIONS

In this chapter, the conclusions from the overall findings are described. After that the critical reflection is presented. Finally, the recommendation for further research is explained.

7.1 CONCLUSIONS

Information security is the protection of information itself as well as its information system to ensure confidentiality, integrity, availability and accountability. Several major roles in organizations are to protect information, to enable the business operations, to provide a safeguard platform for applications and to guard technology assets. Therefore there is a need to ensure a proper level of information security.

To do this, the security risk management should be implemented. The five phases presented are risk analysis, risk assessment, strategy selection, cost-benefit analysis and implementation. First, assets, threats and vulnerabilities of the IT systems are identified in the risk analysis which supports analysts in identifying possible IT-security incidents. Second, to conduct quantified return on information security investment, the impact and the likelihood served as main inputs to conduct ROISI are quantitatively assessed in the risk assessment. In this phase, uncertainty is possibly assessed as well. Third, not only can risks be mitigated, but also they can be handled by the other strategies namely acceptance, avoidance, and transference. A proper strategy is selected in the strategy selection phase. Note that the selection strategy process is out of scope and the model of ROISI is mainly developed for the risk mitigation strategy. Fourth, an information security investment is assessed by applying the cost-benefit analysis. Fifth, the implementation phase is conducted when results from ROISI are favourable. Since security risk management process is continuing process, the evaluation part for residual risks gives a loopback to the first phase. To conclude this, the whole procedures of security risk management are illustrates in the figure 26 below.

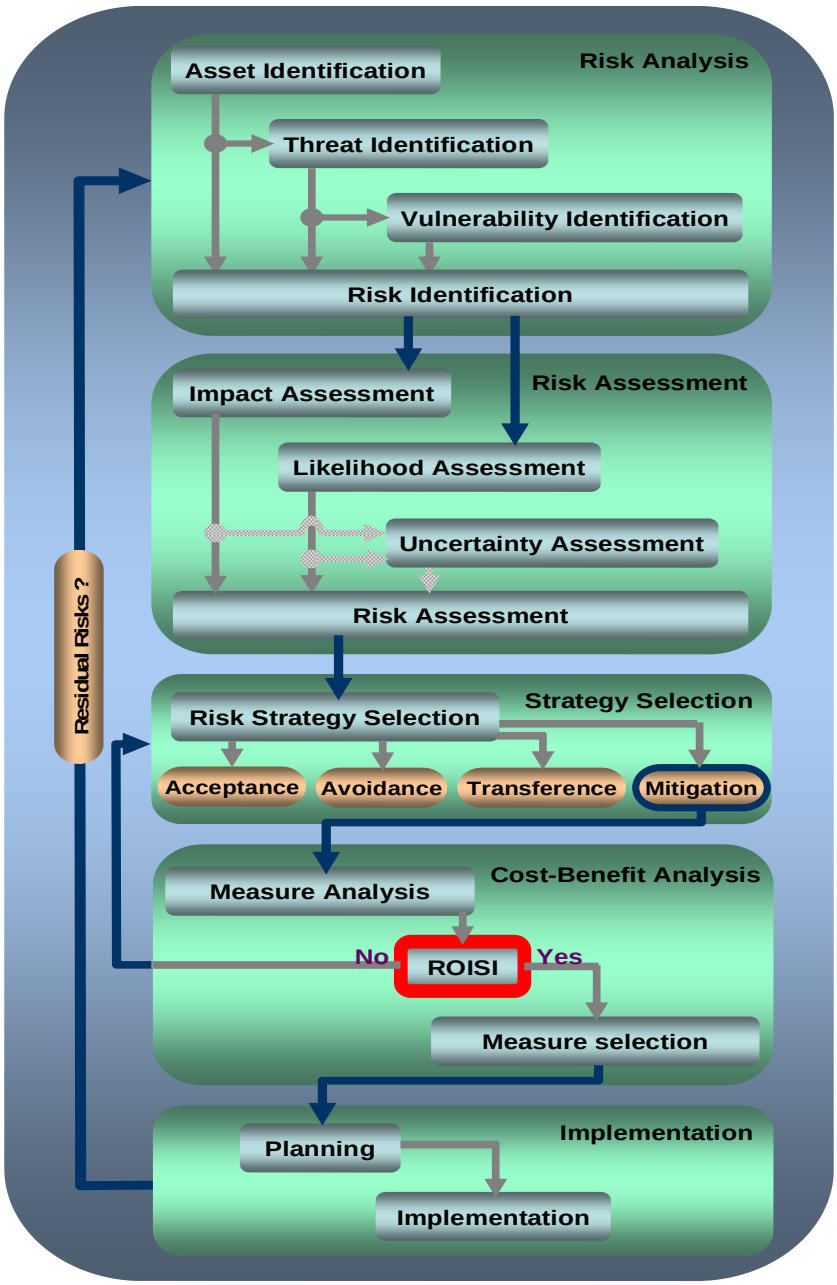


Figure 26: The ROISI position in security risk management process

When an information security investment has to strike with other business opportunities, assessing the investment in numeric terms has become more favourable in the fourth phase of the security risk management. Abbreviated from Return on Information Security Investment, ROISI is an approach assessing an information security investment employing cost-benefit analysis. To conduct the quantitative cost-benefit analysis for an information security investment, the main inputs are an information security investment's numeric benefits and costs. First the benefit can be computed from the difference of loss with and without a security investment. To start this, two main approaches can be applied to quantify

risks. When risk can be acceptably defined as a product of the likelihood and the impact, many experts agree to apply the ALE methodology. Security risk can be measured from the ALE representing the annually expected financial loss. From the impact assessment determining the consequence of a risk, the *Single Loss Exposure* or the SLE can be indicated. The impact of an IT-security incident can be derived from lost revenue, regulatory penalties, lost productivity and reputation loss. Due to the project scope, lost productivity and reputation loss are excluded. For lost revenue and regulatory penalty, the important elements which can be quantified are loss of sale, damage to asset, cost of recovery for software, hardware, internal employee and external consultant, and regulatory penalty. From the likelihood assessment determining the risk's occurring frequency, the *Annual Rate of Occurrence* or the ARO is indicated.

Additionally the second approach conducting the quantitative risk assessment applies from the qualitative technique. The impact and/or likelihood level of a risk can be classified into several levels such as low, medium and high and then these levels are assigned a numeric value for their expected loss and/or frequency. A risk-level matrix could be developed to assess information security risks. From here the SLE, the ARO and therefore the ALE are numerically identified.

Next, the costs of controls are divided into the set-up cost (CAPEX) and the recurring cost (OPEX). The set-up cost is expenditure paid to design, establish and start using an information security system, while the recurring cost is annual expenditure recurred to maintain the system operating. The set-up cost consists of software, license fee, hardware, consultancy on analysis and configuration, training and facility, whereas the recurring cost consists of support and maintenance fee and human resource for monitoring.

With the numeric results of the cost and the benefit, there are three popular approaches to execute ROISI namely the ROI/ROISI, the NPV and the IRR. In this research, another approach called the discount ROISI or the dROISI is developed by combining the NPV and the ROISI. The popularity of the ROI approach and the reliability of the NPV are used as a stand point to compensate the weak point of the ROI, which does not take into account the time value of money. The concept is rather simple but it may take some times before decision makers will accept it due to its novelty.

Table 20: The comparison for all approaches

Approach	ROI/ROISI	dROI/dROISI	NPV	IRR
Magnitude	No	No	Yes	No
Time value of money	No	Yes	Yes	Yes
Complexity	Low since not taking into account time value of money	Medium/High – since it needs the rate of return for each period but its concept is simple	High – since it needs the rate of return for each period	High – difficult to manually calculate but easier with computer calculation
Popularity (Due to the CSI survey)	High since it is rather simple	-	Medium	Medium/Low
Comment	Less reliable than the other approaches	More reliable than the ROISI approach and Sensitive to the time value of money	the only method indicating the magnitude; however, sensitive to the time value of money	doubtful assumption: the whole period has the same rate of return

In the case that decision makers prefer to know *quickly* information on the effectiveness of their invested money, the ROI/ROISI is the best option. In the case that decision makers prefer to know *reliable* information on the effectiveness of their invested money, the dROI/dROISI is the best option. In the case that decision makers prefer to know the magnitude information of their invested money at the present value, the NPV is the best option. In the case that decision makers prefer to compare the rate resulted from an investment to the other rate(s) for instance an interest rate or the company's hurdle rate, the IRR is the best option. However the time value of money has limited information; therefore, all methods using it may face this disadvantage towards the use of the methods alone. Overall, a decision maker should use a combination of methods to justify investment opportunities in order to compensate weaknesses of individual method and to have a better picture of the investment(s).

Combining the benefits and the costs, the relation between IT-security incidents and their impacts can be modelled to conduct the quantitative cost-benefit analysis for information security investment in the way presented in the figure 27 below.

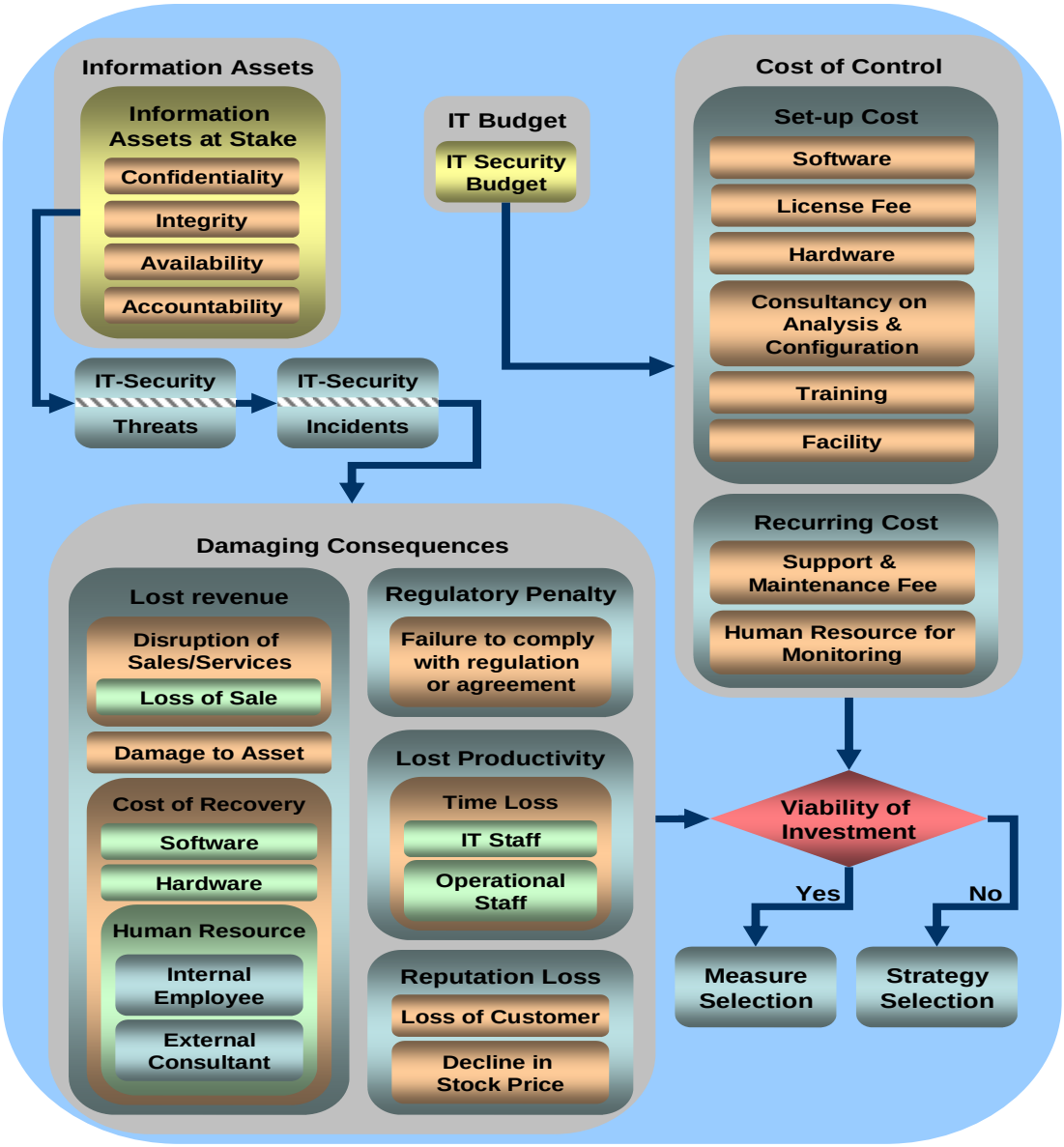


Figure 27: The model for return on information security investment

Starting from a company possessing valuable information assets, some information assets are at stake. These assets are endangered by IT-security threats and if the threats are materialized to be incidents, this will cause damaging consequences to the company. As a part of IT budget, IT security budget can be used for establishing and maintaining an information security system with the costs explained earlier. The viability of an investment can be tested with the benefits against the costs.

Even though lost productivity and reputation loss are out of scope of this research, a guideline for companies and other researchers is that lost productivity may possibly be derived from time loss of IT and/or operational staffs and reputation loss may possibly be

derived from loss of customers and/or decline in stock price. However this should be studied in greater details.

According to these two models, an ROISI application is developed as presented in chapter 5. The conclusions from evaluating the models and the application is that according to experts' interviews, the models are rather practical, good, clear and useful. The uncertainty assessment part in the security risk management model is somewhat crucial and beneficial even though it could be hard and time-consuming when implementing it. Next, since the application gets very positive feedbacks, especially with the detailed risk assessment analysis, it can be concluded that it is fairly good quality, practical, useful, generic and presentative. The difficulty to eventually complete the analysis mainly comes from two sources. One is analysts seem to have a trouble in understanding the financial terms. The other is lack of information about the likelihood and the impact of IT-security incidents. Please note that even though the models and the application are developed based on the findings from literature, the generalization of the research results may possibly be influenced by TNO culture and environment.

Lastly, since the return on information security investment relies on expert estimation which needs to deal with uncertainty, here we conclude the ways to support this. First of all, for the impact, disaggregation, which splits an estimate into smaller elements, is applied to help experts to give better estimates for the impact. However it is still recommended to give an expert feedback and training and to combine more than one expert's opinions (multiple-expert estimate) to reduce bias and increase reliability. Second, for the likelihood, the Monte Carlo method may be one of other alternatives to be applied to provide more information about the results to decision makers. Please note here that the Monte Carlo approach could not only apply to the likelihood, but also other variables as well, for instance the forecasted discount rate. Even though the approach is useful to have a better picture of the possible results, the Monte Carlo approach is still doubtful whether it is practically beneficial for a company to use it. This is because it requires additional information from experts to describe the likelihood's uncertainty like range, mean, standard deviation or distribution pattern, which could be very time consuming. Additionally there is often still not much information about the distribution of the likelihood. Because of several above reasons, we would like to conclude here that in a case that complexity is low and experts have knowledge of probability distribution, it is worthwhile to apply the Monte Carlo approach. On the other hand, in a case that complexity is high and experts' degree of belief is low, we do not recommend a company to apply the Monte Carlo approach to ROISI. Generally an ROISI case is rather complex and its size is large; it may not be useful to apply the Monte Carlo approach to this model due to our knowledge. However more researches can study the application of the Monte Carlo approach in the ROISI issue in detail. Finally, for overall results, sensitivity analysis can be applied to support decision makers to better understanding the model structure and the main sources or inputs of model output uncertainty.

In the next section, several points are addressed to critically reflect this research.

7.2 REFLECTION

CONTENT-WISE

In the chapter 2 and 3, a book from Whitman and Mattord called "Principles of Information Security" was greatly used; this may somewhat have an influence on the result of the thesis. However the chapter 2 is basically provided for readers to sufficiently have basic knowledge of information security. The core knowledge building the models and the application is taken from literature presented in the chapter 3, 4 and 5. In the chapter 3, the main model is derived from several international standards, a couple of books and a number of scientific articles. As a result, inputs from this book will not much directly impact results from the whole research.

Another important point reflecting the results of this research is contextual factor. As we mentioned earlier, contextual factors may influence decision making (Cheng and Levitt 2000). As a result, the effectiveness of the models and the application partially depend on situations or contexts they applied in.

When we reflect on the application, there are several limitations of the application. The *first* limitation is that the application may not be suitable to all different cases; it needs adjustments when being applied to some specific cases in order to better fit in different situations. For instance, if the application is applied to a hospital case, loss of life most likely becomes more important element than loss of sale, damage to asset and cost of recovery in the application when assessing the return on information security investment. The *second* limitation is that the application is designed for maximum ten controls, five assets and two depreciation methods over a period of five years since it is the first edition. Currently the application can manually be expanded but its expandability can definitely be improved by using Macro in Microsoft Excel or even the same type of application can be developed on other programmes and/or other platforms. The *third* limitation is that this application cannot be used by any not-specialized person because it should be filled in by experts who can obtain relevant technical knowledge and business information to prevent any *garbage in-garbage out* situation, meaning that when unreliable information is filled in the application, results from the application, as a result, are not trustable as well. Financial understanding is important for decision makers.

Another point when reflecting the usage of the application is actor behaviour. This point is rather important because information about risk of information security is very sensitive. When looking at decision making processes, there are different levels of decision makers (individual, group, organization and inter-organization) and approaches. Several possible approaches for different levels are for example rational or analytic perspective (bounded rational and satisficing) and political, irrational or strategic perspective (incrementalism or 'muddling through', 'humble' decision-making or 'mixed scanning', garbage can model, game approach, stream model and round model) (Koppenjan and Klijn 2004; Groenleer 2009). As a result, users or any stakeholders related to the use of the application may use their strategic behaviour and try to influence the results. This is because the use of this application is resided in multiple-actors environment with different preferences, interests, perceptions,

and expectations. It is not always the case that actors involved solve a problem through scientific analysis and goal-oriented processes.

When realizing this in the framework between a consultancy company and a client company, an individual, for instance a manager responsible for information system in the client company, may feel uncomfortable to reveal problems or weaknesses within his (or her) responsibilities and therefore not tell the consultancy company the best estimates according to his knowledge. On the other hand, an individual from the consultancy company may want to exaggerate a return on investment that the client company will receive from the consultancy company. This example shows that realizing actor behaviour can help to be aware of *garbage in-garbage out* situations.

The last point to reflect here is the evaluation part of the research. Derived from the models built from a number of literatures, the application generates "crisp" numeric results. Due to the time limitation, the research results were not validated by conducting case study and the evaluation part was limited. Nevertheless we conducted a brief evaluation in order to get the feeling whether the models seem right and the application is feasible and practical or not. However, from our point of view, this is not sufficient to actually critically evaluate the results of the research due to insufficient time available. Besides from evaluating, validating is needed as well. If we had conducted case study for several cases, we would have been able to confirm or disconfirm and to be more explicit about types of cases that are suitably applied our results and other information when using them in practice. As a consequence, the models and the application still should be critically evaluated and should be validated.

PROCESS-WISE

The whole process of this research has been conducted for about 5-6 months. To reflect this, the period of 5-6 months is very little for a research in the area of ROISI, especially when the models and the application were developed. This research closely involved several people from both Delft University of Technology and TNO ICT. Many activities had been planed much in advance to avoid any possible delay. Regular meetings are scheduled with two supervisors (the first supervisor and the TNO supervisor) to keep track of the research and to have discussions on several topics from both business and academic perspectives. However it may be wise to schedule several meetings with the second supervisor, while conducting the research. This is because he has different expertises from the first supervisor and we could have another insight from different perspective which would be beneficial for the research.

To reflect on the evaluation process, when we conducted the interviews to get experts' opinions on the models, due to time availability we did not have any other comparable models for experts to weigh against the ones we presented in this paper. This may limit their scope of judgement since they do not have any alternatives. However we attempted to criticize our models and asked the experts some detailed questions. This might help us to stimulate the experts to consider several different aspects.

7.3 RECOMMENDATION FOR FUTURE RESEARCH

Previous section concludes the whole research; however, there are rooms to fulfil, enhance and confirm this research knowledge. For further researches, several suggestions are presented in this section. *First*, it is interesting and very valuable to explore the way how a company should select a suitable strategy to cope with risks as a part in the security risk management. It may be more realistic to apply context-based decision making methods. *Second*, in the application the ARO is assumed to be constant over the period of indicated time; however, the ARO is varied over a 5-year period as shown before. It is another interesting point to investigate how the variety of the ARO should be realized in the application while keeping the complexity at the practical level. *Third*, from the last point we reflected, due to the limited time in the evaluation part, we could not actually validate the results and the results could not be critically evaluated. Future researches can apply the case study approach to test whether the models and the application are valid or not. The case study yields much more intense insight than conducting interviews. *Fourth*, when information about the likelihood of IT-security incidents is available, further researches can investigate the way how the Monte Carlo approach should be applied properly. For instance, what is the most important information needed for the probability distribution? What is the optimal level between accuracy and complexity? *Fifth*, from the critical reflection, as we realize actor behaviour that they may behave strategically and even in a worse case they may misuse the models and the application, future researches can study in detail on actor behaviour. For instance, the questions are how actors involved in ROISI are modelled, what the impacts are from their behaviour in different scenarios, how the application will be used, which factors impact the use of the models and the application, how to improve transparency of the application to prevent actors misuse it, and which kind of safeguards should be developed. *Sixth* and last, the sensitivity analysis is included as one of the approached we can handle uncertainty; however, we had no time to apply the sensitivity analysis into the application developed. Several possible questions for future researches are how to integrate a sensitivity analysis into the ROISI model and application, should we use all inputs of the ROISI application as inputs for the analysis, if not, which inputs of the ROISI application are important and suitable to use as the analysis' inputs and how the results of the sensitivity analysis should be interpreted, for instance.

To lastly sum up, with all these understanding about information security, security risk management, cost-benefit analysis, and other relevant knowledge, the results of this research can fulfil the need of a better model to depict the relation between IT-security incidents and their negative consequences in order to conduct the cost-benefit analysis that deals with uncertainty for the real world of information security. Please note here that the models and the application are a first attempt in making a true quantitative model but in order to make the models and the application more accurate and more useful in practice, it still needs further researches.

APPENDIX

A. DELFT UNIVERSITY OF TECHNOLOGY

Delft University of Technology is not only the oldest, but also the largest university of technology of the Netherlands. Its research and education is of this unique institution top-ranked. TU Delft was founded in 1842 as the Royal Academy by King Willem II. It has been known as the Delft University of Technology (TU Delft) since 1986. A short summarized history of TU Delft is as follows:

- Royal academy: 1842 – 1864 by King Willem II
- Polytechnic school: 1864 - 1905
- Institute of Technology: 1905 - 1986
- Delft University of Technology: 1986 - present

This research is conducted to fulfil the requirements for the degree of Master of Science in the subject of Management of Technology at the section of Information and Communication Technology in the Infrastructure Systems and Services department at TU Delft.

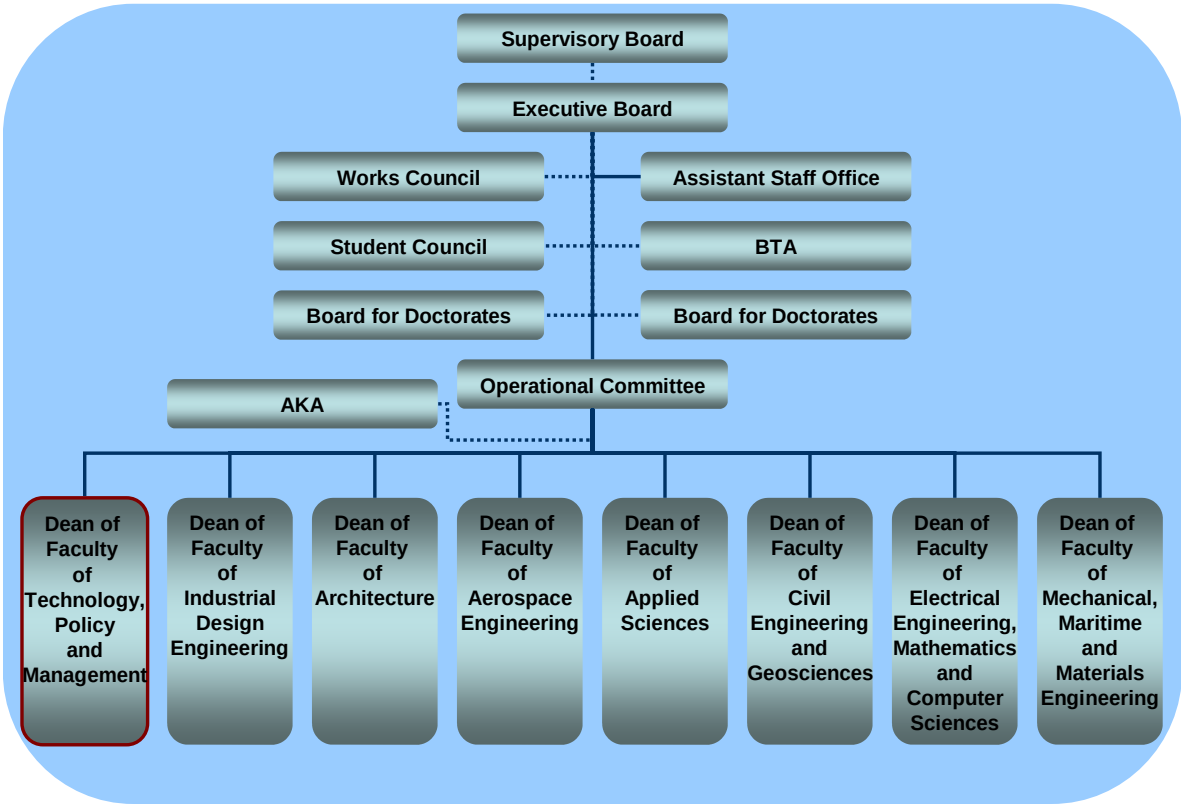


Figure 28: The position of the faculty of Technology, Policy and Management in TU Delft's organogram

The figure 28 illustrates the position of TPM faculty in TU Delft and the next figure illustrates the ICT section in this faculty.

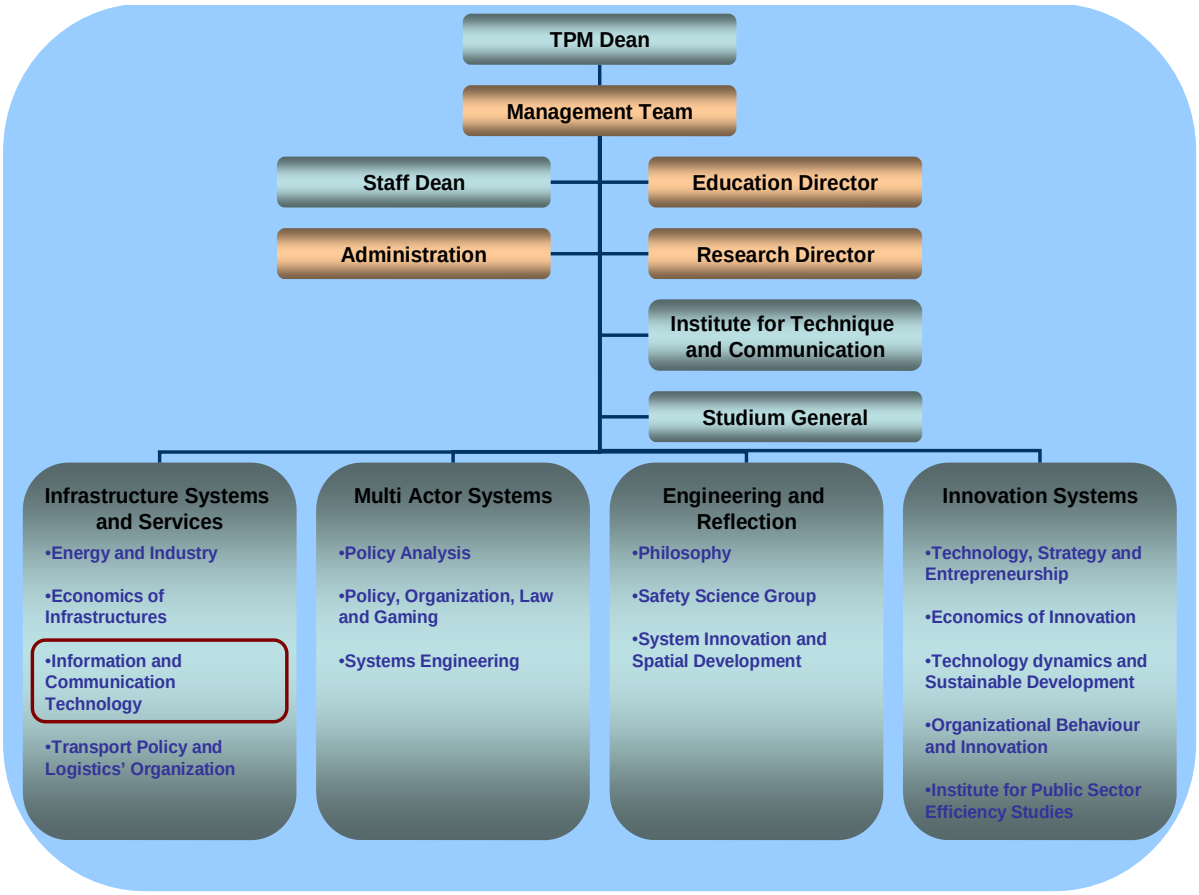


Figure 29: The position of the ICT section in TPM

Source: www.tudelft.nl and www.tbm.tudelft.nl

B. NETHERLANDS ORGANIZATION FOR APPLIED SCIENTIFIC RESEARCH

Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek or Netherlands Organization for Applied Scientific Research (TNO) is a not-for-profit organization that focuses on applied science in the Netherlands. TNO is a knowledge-based organization for companies, government and public organizations. TNO conducts research and provides consultancy services as well as grants licences for patents and software. TNO tests and certifies products and services. By law, TNO was founded in 1932 to drive technology development to support companies and governments with innovative, practicable knowledge in the Netherlands.

The research is conducted in TNO Information and Communication Technology, Business Unit: Innovation Management, Sub-Unit: Strategy Business Analysis in collaboration with Business Unit: Information Technology, Sub-Unit: Security. The two following figures illustrate TNO's organogram and the position of the Strategy Business Analysis sub-Unit.

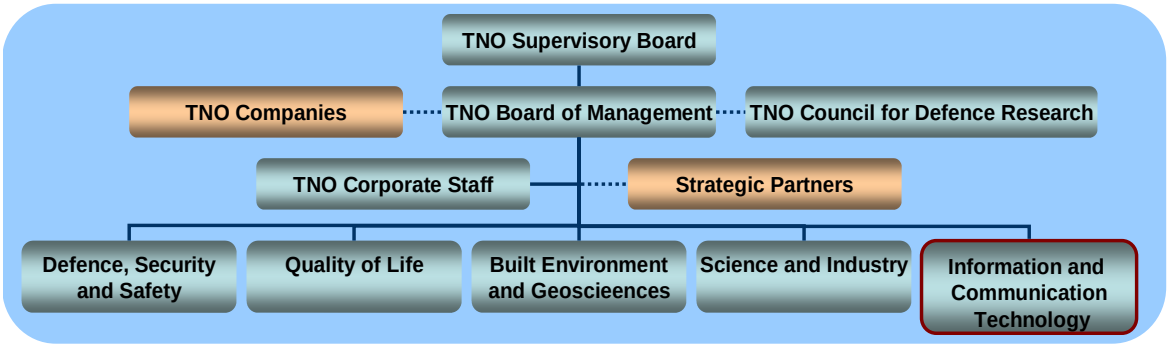


Figure 30: The position of ICT in TNO's organogram

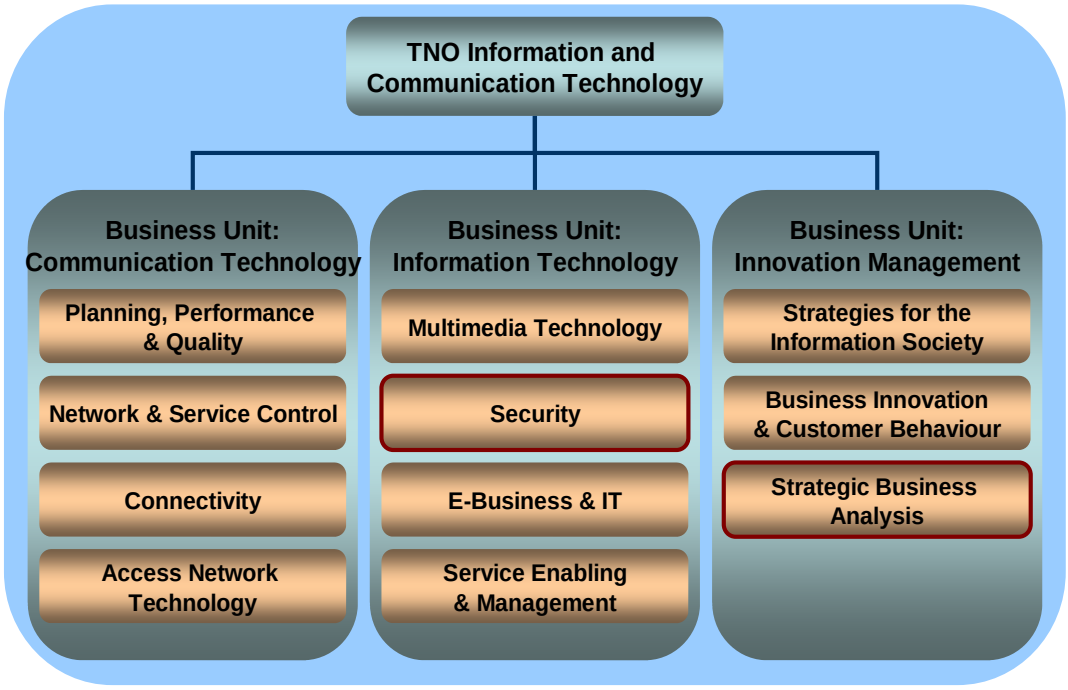


Figure 31: The positions of the Strategic Business Analysis and Security sub-units in TNO ICT

Source: en.wikipedia.org/wiki/TNO, www.tno.nl and nieuwspunt.ict.tno.nl (intranet)

C. QUANTIFYING LIKELIHOOD AND COSTS OF INCIDENTS (LOCKSTEP 2004)

The basis for these frameworks is the likelihood and impact definitions from the ACSI 33 Risk Assessment method (ACSI 33 2000). The likelihood of an IT-security incident is classified into seven levels, from "Negligible" to "Extreme". Defined in (ACSI 33 2000), the levels are quasi-quantitatively. Lockstep quantifies the quasi-quantitative values to estimated numbers

Table 21: The quantification of qualitative likelihood based on ACSI 33

Likelihood	Description from ACSI 33	Numeric value
Negligible	Unlikely to occur	**0.05***
Very Low	Likely to occur two/three times every five years	**0.5**
Low	Likely to occur once every year or less	**1.0**
Medium	Likely to occur once every six months or less	**2.0**
High	Likely to occur once per month or less	**12.0**
Very High	Likely to occur multiple times per month or less	**50.0**
Extreme	Likely to occur multiple times per day	**500.0**

* Note that Lockstep takes an advice from OICT to assign the numeric value of the "Negligible" a rate of once per 20 years.

Source: A Guide for Government Agencies Calculating Return on Security Investment from Lockstep.

D. THE DISCOUNT RATE OR OPPORTUNITY COST OF CAPITAL

The discount rate is needed to be filled in the application in order to calculate the dROISI and the NPV for the results of the financial return. The discount rate presents a rate that decreases value of money by inflation or other factors. There are several possibilities. Some companies use a rate from Weighted Average Cost of Capital (WACC), while some use an interest rate charged by a bank. Some other companies set a 'hurdle rate', 'minimum acceptable rate of return', or 'cutoff rate', which is the minimum required rate of return on an investment for a company. This rate generally is higher than the other rates. Which rate will be used depends on the culture and decision made by a company.

WEIGHTED AVERAGE COST OF CAPITAL (WACC)

In case that a company prefers to use WACC method for the discount rate, the company should calculate a company WACC. This company WACC is based on the company's financial capital structure. The figure below shows an example calculating WACC adapted from (Neuhaus 2008):

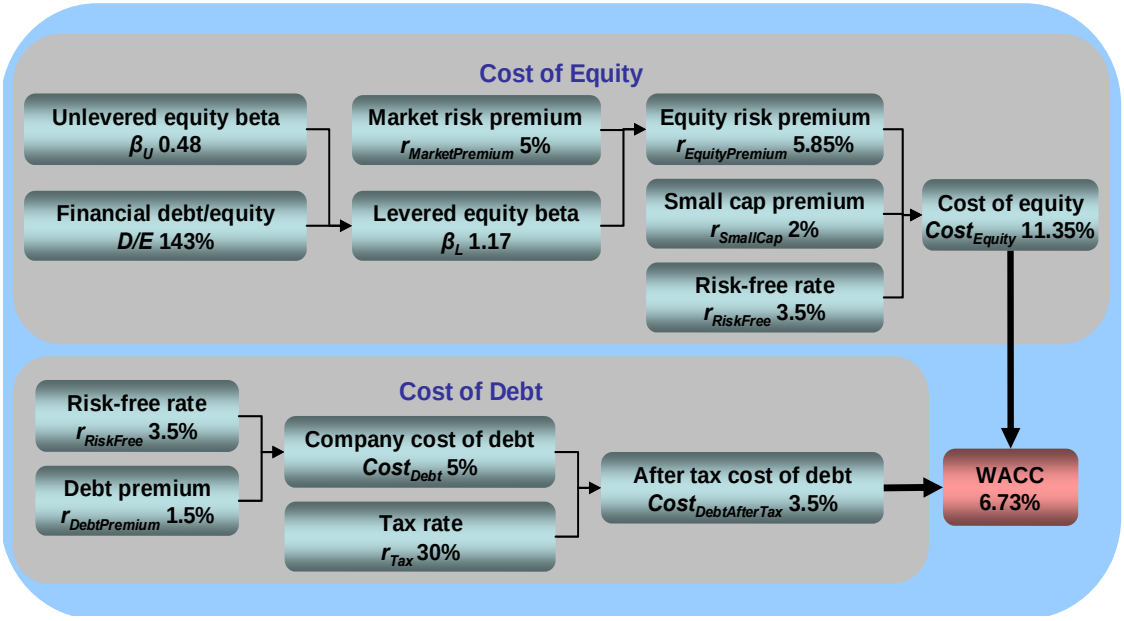


Figure 32: A sample of WACC calculation

Where, beta (ß) measures the volatility of a security compared to the market as a whole. Unlevered equity beta ($ß_U$) is beta with an equity ratio of 100% (or without impact of debt). Financial debt/equity is an optimal long-term capital structure. Levered beta ($ß_L$) is unlevered beta (1 + (Debt / Equity)). Market risk premium is long-term average of the deviation of the return of risk free bonds in comparison to the return of the stock market. Small cap premium is premium for small capitalized companies, which is based on empirical studies by Ibbotson. Lastly, risk-free rate is yield of long-term government bond, normally 10-20 years. Several rates are assigned as follows:

Unlevered equity beta ($ß_U$) = 0.48, Financial debt/equity (D/E) = 143%, Market risk premium ($r_{MarketPremium}$) = 5%, Small cap premium ($r_{SmallCap}$) = 2%, Risk-free rate ($r_{RiskFree}$) = 3.5%, Debt premium ($r_{DebtPremium}$) = 1.5% and Tax rate (r_{Tax}) = 30%. Please note that these assigned rates generally depend on an industry a company operates, a structure of the company itself and a country the company resides.

The formulas and calculations of WACC are shown as follows:

$$\beta_L = \beta_U * \left(1 + \frac{D}{E}\right)$$

$$1.17 = 0.48 * (1 + 143\%)$$

$$r_{EquityPremium} = \beta_L * r_{MarketPremium}$$
$$5.85\% = 1.17 * 5\%$$

$$Cost_{Equity} = r_{RiskFree} + r_{SmallCap} + r_{EquityPremium}$$
$$11.35\% = 3.5\% + 2\% + 5.85\%$$

$$Cost_{Debt} = r_{RiskFree} + r_{DebtPremium}$$
$$5\% = 3.5\% + 1.5\%$$

$$Cost_{DebtAfterTax} = Cost_{Debt} * (1 - r_{DebtPremium})$$
$$3.5\% = 5\% * (1 - 30\%)$$

$$WACC = \frac{Cost_{Equity} + \left(Cost_{DebtAfterTax} * \frac{D}{E} \right)}{\left(\frac{D}{E} + 1 \right)}$$
$$6.73\% = \frac{11.35\% + (3.5\% * 143\%)}{(143\% + 1)}$$

Source: Corporate Finance - Business valuation and Value management from Markus Neuhaus, Swiss Federal Institute of Technology Zurich.

REFERENCE

A. Mosleh; V.M. Bier and G. Apostolakis (1988). "A critique of current practice for the use of expert opinions in probabilistic risk assessment." Reliability Engineering and System Safety.

A. Saltelli, S. T. F. C. a. M. R. (2004). "Sensitivity analysis in practice: a guide to assessing scientific models."

ACSI 33 (2000). Risk Management Handbook 3, Australian Communications - Electronic Security Instruction 33 V1.0 D. S. Directorate.

Anderson, R. (2001). Why information security is hard: An economic perspective. Proceedings of the seventeenth annual computer security applications conference.

Anderson R.; and Schneier B. (2005). "Economics of information security." IEEE Security and Privacy.

Berg J. van den and Pijl G. van der (2004). Security and ICT Audit 2004/2005.

Berinato, S. (2002). "Finally, a real return on security spending." CIO Magazine.

Böhme R. and Kataria G. (2006). Models and measures for correlation in cyber-insurance. The fifth workshop on the economics of information security.

British Standard 7799-2:1999 (1999). Information Security Management.

British Standard_7799 (1996). Information Security Management.

Carol H. Cheng and Raymond E. Levitt (2000). "Modelling contextual decision making in service organizations." Stanford University.

Cas de Bie (2005). Exploring way to model reputation loss. Economics. rotterdam.

CERT (2007). "Computer Emergency Response Team Coordination Center (CERT/CC) vulnerability remediation statistics."

Chan, S. (2001). "Risky E-Business." Internal auditor.

Christopher J. Alberts and Audrey J. Dorofee (2002). Managing information security risks: the OCTAVE approach, Addison-Wesley.

Conrad, J. R. (2005). "Analyzing the Risks of Information Security Investments with Monte-Carlo Simulations." IEEE Computer Society.

D. Vose (2000). "Risk Analysis - A Quantitative Guide." West Sussex, England: John Wiley and Sons.

Daniel Mellado a; Eduardo Fernández-Medina and Mario Piattini (2007). "A common criteria based security requirements engineering process for the development of secure information systems." Computer Standards & Interfaces **29**: 244-253.

Deng Z. Y. and Zeng G. X. (1989). Application of Analytic Hierarchy Process (AHP) on Intension Characteristic and Analytic I and II, National Statistics Report.

Denning, D. (2000). "Reflections on cyberweapons controls." Computer Security.

Dictionary.com (Retrieved July 17, 2009). uncertainty. The American Heritage® Dictionary of the English Language. F. Edition.

Do Hoon Kim; Taek Lee; and Hoh Peter In (2008). Effective Security Safeguard Selection Process for Return on Security Investment. IEEE Asia-Pacific Services Computing Conference.

George T. Friedlob and Ralph E. Welton (2008). Keys to Reading an Annual Report, Barron's Educational Series.

Gordon A. L. and Loeb P. M (2006). Managing cybersecurity resources: A cost-benefit analysis, McGraw Hill.

Gordon A. L. and Loeb P. M. (2002). "The economics of information security investment." ACM.

Gordon A. L. and Richardson R. (2004). "The new economics of information security." Information Week.

http://en.wikipedia.org/wiki/Depreciation#Declining-Balance_Method.

http://en.wikipedia.org/wiki/Depreciation#Straight-line_depreciation.

http://www.investorwords.com/4372/salvage_value.html.

Huseyin Cavusoglu; Birendra Mishra; and Srinivasan Raghunathan (2004). "A Model for Evaluating IT Security Investments." COMMUNICATIONS OF THE ACM.

ISF (2005) ROSI - Quick Reference Guide.

ISO/IEC 27001:2005 (2005). "Information technology-Security techniques-Information security management systems-Requirements."

ISO/IEC TR 13335-1 (1996). "Information technology - Guidelines for the management of IT Security - Part 1: Concepts and models for IT Security."

ITU (2008). ITU World Telecommunication/ICT Indicators Database.

J.F.M. Koppenjan and E. H. Klijn (2004). Managing Uncertainty in Networks, Routledge.

J.H. Halton (1970). "A retrospective and prospective survey of the monte carlo method." SIAM Review.

James B.D. Joshi; Walid G. Aref; Arif Ghafoor; and Eugene H. Spafford (2001). "Security Models for Web-based Applications." COMMUNICATIONS OF THE ACM.

Kevin Buck; Prasant Das and Diane Hanf (2008). "Applying ROI Analysis to Support SOA Information Security Investment Decisions." IEEE.

Knight, F. H. (1921). "Risk, Uncertainty, and Profit."

Koen Yskout; Thomas Heyman; Riccardo Scandariato; Wouter Joosen (2006). A system of security patterns. R. CW469.

Lockstep, C. (2004). A Guide for Government Agencies Calculating Return on Security Investment.

M. Krause and H. F. Tipton (1999). "Handbook of Information Security Management." Auerbach Publications.

Markus Neuhaus (2008). Corporate Finance, Swiss Federal Institute of Technology Zurich.

Martijn L.P. Groenleer (2009). Decision-making, MoT1450, Faculty of Technology, Policy and Management, Delft University of Technology.

Martin Jagels and Catherine E Ralston (2006). Hospitality Management Accounting, John Wiley and Sons.

Michael E. Porter and Victor E. Millar (1985). "How Information Gives You Competitive Advantage: The Information Revolution Is Transforming the Nature of Competition." Harvard Business Review.

Michael E. Whitman and Herbert J. Mattord (2008). Principles of Information Security, Thomson Course Technology.

Muhammad Al Humaigani and Derrek B. Dunn (2004). "A model of return on investment for information system security."

NIST (2002). Risk Management Guide for Information Technology Systems. 800-30. N. I. o. S. a. Technology.

NIST Special Publication 800-100 (2006). Information Security Handbook: A Guide for Managers: Recommendations of the National Institute of Standards and Technology. D. o. Commerce.

OCC (1998). "Technology rsik management: PC banking." Office of the comptroller of the Currency.

Park, Chan S. (2007). Contemporary Engineering Economics (4th Edition). Prentice Hall. p. 216. ISBN0-13-187628-7

Pathak, J. (2005). "Information Technology Auditing - An Evolving Agenda." Springer Verlag.

R. L. Krutz; R. D. Vines; and E. M. Stroz (2001). "The CISSP Prep Guide: Mastering the Ten Domains of Computer Security." Wiley Publishing.

Ratto M.; Tarantola S. and Saltelli (2001). "Sensitivity analysis in model calibration: GSA-GLUE approach."

Rebecca T. Mercuri (2003). "Analyzing Security Costs." Communications of the ACM.

Robert Richardson (2008). CSI Computer Crime & Security Survey.

Rok Bojanc and Borka Jerman-Blažič (2007). "Towards a standard approach for quantifying an ICT security investment." Computer Standards & Interfaces.

Rok Bojanc and Borka Jerman-Blažič (2008). "An economic modelling approach to information security risk management." International Journal of Information Management.

Schechter S. E. (2002). Quantitatively differentiating system security. The first workshop on economics and information security (WEIS)

Schneier, B. (2004). "Secrets & lies, digital security in a networked world." Wiley Publishing.

Shaw, G. (2005). "Identity Theft: Managing the Rsik." Insight Consult.

Shawn A. Butler (2003). "Security Attribute Evaluation Method." CMU-CS-03-132.

Stefano Bistarelli; Fabio Fioravanti and Pamela Peretti (2006). Defense trees for economic evaluation of security investments. First International Conference on Availability, Reliability and Security (ARES'06), IEEE.

Theodosios Tsiakis and George Stephanides (2005). "The economic approach of information Security." computer and security, Elsevier.

Thomas Neubauer; Markus Klemen; and Stefan Biffl (2005) Business Process-based Valuation of IT-Security.

Thomas R. Peltier (2005). "Information Security Risk Analysis." CRC Press.

Zegers, N. (2006). "A Methodology for Improving Information Security Incident Identification and Response."