DATA ENVELOPMENT ANALYSIS APPLIED TO THE SECURITY OF IT BASED INFORMATION SYSTEMS

DIPLOMA THESIS

Patrick Rueegg
Quinjenje, Angola

Institute of Computer Science

University of Zurich
Prof. Dr. Gerhard Schwabe

Supervisor
Jürg Brun, ERNST & YOUNG

Submission Date 1st January 2006
Matriculation Number 95-914-008

ABSTRACT

The measurement of the efficiency of securing information technology (IT) based information systems is a very difficult undertaking, but could aid the promotion of a better understanding of the key factors involved in the security of IT based information systems. First of all a general understanding of what security means to IT based information systems will be established and a model of the security process will be developed.

Data Envelopment Analysis (DEA) is a linear programming based technique for measuring the relative performance of business processes where the presence of multiple inputs and outputs makes comparisons difficult. After modeling the security process this work focuses on the potential use of DEA in the field of security of IT based information systems.

It is shown that DEA is a practical tool and helps to better understand the security process. Potential best practices are concluded from the results and it is argued that compliance to laws, business strategy alignment and security policies help to increase the protection of IT based information systems.

The models and ideas developed motivate for further research in the field of IT based information systems combined with DEA.

KURZFASSUNG

Es ist ein ziemlich schwieriges Unterfangen, die Effizienz zu messen, mit welcher ein elektronisches Informationssystem gesichert wird. Ein solches Unternehmen könnte sich aber dennoch lohnen, da man dadurch eventuell ein besseres Verständnis über die in der Sicherheit von elektronischen Informationssystemen involvierten Faktoren erhält. Zuallererst wird ein Verständnis über die Bedeutung von Sicherheit im Umfeld von elektronischen Informationssystemen erarbeitet. Danach wird ein Modell des so genannten Sicherungsprozesses entworfen.

„Data Envelopment Analysis“, auch kurz DEA genannt, ist eine in der linearen Programmierung benutzte Methode um Leistungen relativ zu messen. Dieses Vorgehen wird dann angewendet, wenn mehrere verschiedene Eingangsleistungen und Ausgangsprodukte vorhanden sind und somit Leistungsvergleiche problematisch sind. Nach dem Erstellen des Modells des Sicherungsprozesses wird untersucht, inwieweit sich DEA im Bereich der Sicherheit von elektronischen Informationssystemen anwenden lässt.

Es hat sich gezeigt, dass DEA in der Praxis anwendbar ist und hilft, den Sicherungsprozess besser zu verstehen. Es werden mögliche beste Handlungsweisen hergeleitet und argumentiert, dass die Befolgung von Gesetzen, die Berücksichtigung der Geschäftsstrategie sowie klare, strukturierte Verfahrensweisen bezüglich der Sicherheit den Schutz von elektronischen Informationssystemen erhöhen.

Die entwickelten Modelle und Ideen motivieren weitere Forschung im Bereich der Sicherheit von elektronischen Informationssystemen in Verbindung mit DEA.

ACKNOWLEDGEMENT

My heartfelt thank you for the time invested in this undertaking goes to Jürg Brun from Ernst & Young. He really encouraged me a lot to develop my ideas and we had very constructive discussions. I would also like to thank Prof. Dr. Schwabe of the Institute of Computer Science of the University of Zurich for his support. A thank you goes to Prof. Dr. Mayer of the Institute of Operations Research, University of Zurich, for the very interesting conversations about DEA. I'm also very grateful to Silvia von Bergen. She introduced me into DEA and I got a lot of useful tips from her. With her I could always discuss unconventional ideas. I would also like to thank Laurent Fabre from Ernst & Young, Felix Walz, the security officer from the ETH Zurich, and all others around the world who helped me. A very special thank you goes to my father Willi Rüegg. He has always showed me different and practical aspects of digital information systems. And a big thank you goes to my mother Annemarie Rüegg and especially my partner Sandra Oelhafen for their support and encouragement.

I. TABLE OF CONTENTS

1 INTRODUCTION

Information Technology (IT) is getting more and more accepted as an autonomous but integrated part of the business. As within each area of responsibility the management of the IT organization has to answer to the company's management. The IT management is beholden to quantify the value of IT, to take charge of costs and investments, to name the payback from the use of IT, to serve the company in an effective way and to assess and control IT risks. In particular the IT organization is required to build and maintain a secure information infrastructure. But to appreciate the value IT is contributing to the success of an enterprise is exceedingly difficult, especially to estimate how IT security respectively information systems security conduces to success.

The monetary benefit of the security of IT based information systems is ever so often not to estimate. Other performance metrics have to come into play. For example some firms use balanced scorecards to track IT performance in four dimensions: customer satisfaction, employee satisfaction, management effectiveness and quality[1]. But a business unit's performance is a far more complex phenomenon and the use of single measures ignores the interactions, substitutions or tradeoffs among various performance measures[70]. There is an increasing concern not only to measure individual aspects but to get a broader view indicating the efficient use of resources. Such monitoring would enable the IT organization to look at performance from perspectives relevant to the broader organizational mission.

Monitoring a business process, e.g. securing information systems, is even more challenging because we have multiple inputs and outputs related to different resources, activities and environmental factors[24]. Unfortunately in the majority of cases the functional relationships among the various factors are unknown. Thus the business operations and information systems security respectively are not fully characterized. This makes performance evaluation hardly impossible. Nevertheless with Data Envelopment Analysis (DEA) we can benchmark business processes against similar operations taking multiple inputs and outputs into account, without the need of a priori information on the functional relationships.

DEA is a linear programming based method developed by Charnes, A., W.W. Cooper and E. Rhodes in 1978[21]. It is used to measure the relative performance of processes respectively organizational units where multiple inputs and outputs make process comparisons difficult. This means that it won't calculate the maximal efficiency that is theoretically possible but the best practices. In contrast to a typical statistical approach that is characterized as a central tendency approach evaluating producers relative to an average producer, DEA compares each

producer with only the "best" producers[67]. Because DEA is an empirical orientated technique and requires very few assumptions, this approach has resulted in its use in a number of studies involving efficient frontier estimation in the governmental and non-profit sector, and in the private sector[69]. DEA has been adopted in a wide area and in different industries. In the health care domain, where the measurement of efficiency has been dominated by the application of cost-benefit and cost-effectiveness analyses, DEA shows a new way to assess efficiency[38]. Others adapt DEA to benchmark public libraries[66], web search engines[36] or financial processes[13], to mention a few examples. DEA is a potentially useful technique for measuring production efficiency and is being increasingly used as a management tool for decision making.

Detailed knowledge of the current situation is the basis of decision making. A firm's first obligation is to gather proper information on how the security of IT based information systems is practiced in the organization. There are business consultancies, like Ernst & Young, providing very useful surveys about how organizations protect against IT systems security threats[25]. This "Information Security Surveys" supply the data used to qualify the security production process in the field of IT.

Bringing together DEA and IT systems security and evaluating performance by means of survey data could help to improve business processes for staying competitive. A particular aim is to examine the validity of the results obtained from DEA with the intent to qualify DEA as an efficiency assessment tool in the field of IT systems security. A very general framework will be described in which these issues is and could be discussed further.

2 METHODOLOGY

It is very complex to investigate the performance of securing IT based information systems. To address this multi-layered issue we develop a methodology that leads us to the performance assessment. The next section describes the approach that will be applied to look at IT based information systems security performance and what subjects we have to take into account. Following this it is outlined how the evaluation will be done and what strategy we follow to investigate the application of DEA to the security of IT based information systems.

2.1 APPROACH

There are different points of view exploring the security of IT based information systems. First of all doing a performance analysis implies creating a model. There are three starting points that are the basis the model is built on. At a first glance there is the field of IT based information systems security itself, viewed as a business process. Secondly we have DEA with its own implications and consequences. And third we need some practical experiences in the form of surveys delivering data that can be used to picture current business processes; especially the security process dealing with IT based information systems.

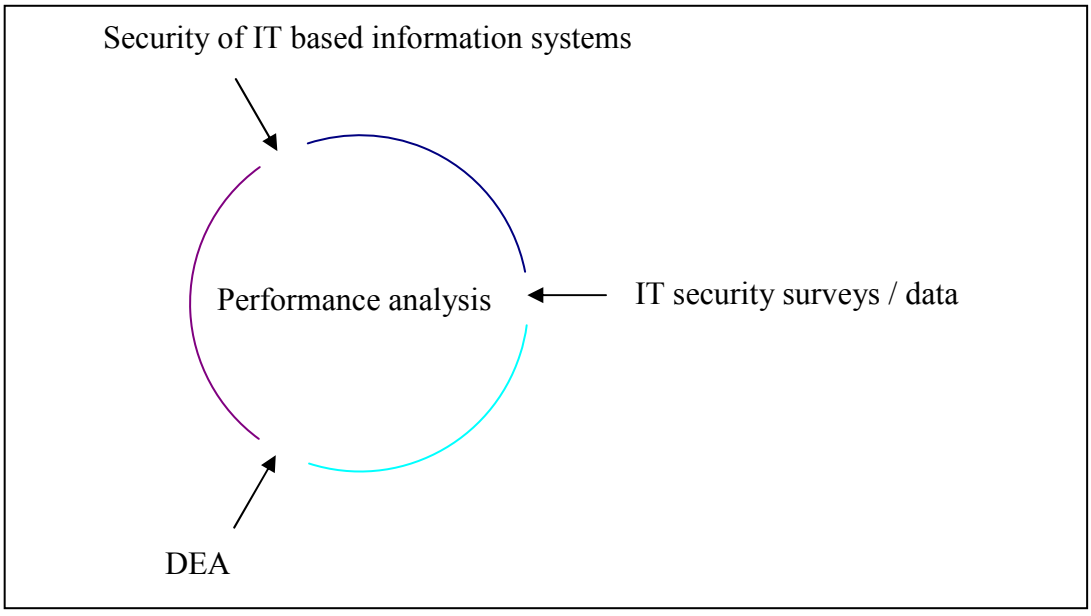

Figure 1: Approach to analyze the security performance of IT based information systems

The next sections describe the afore-mentioned foundation pillars.

2.1.1 THE SECURITY OF IT BASED INFORMATION SYSTEMS

2.1.1.1 INFORMATION SECURITY

Security is a system property and is much more than a set of functions and mechanisms. In today's competitive business environment information, written on paper, stored electronically or spoken in conversation, is constantly under threat from many sources. Indeed, the term "security" should always be viewed in relation to a particular set of threats and assumptions about the environment[51].

Information system security spans the system both logically and physically. The U.S. National Information Systems Security Glossary defines information systems security (INFOSEC) as "the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats"[60].

2.1.1.2 THE SECURITY OF IT BASED INFORMATION SYSTEMS

It is recognized that organizations are becoming increasingly dependent on IT in order to satisfy their corporate aims and meet their business needs. Information systems in form of electronic information systems are an integral part of business operations today.

With the increased use of new technology to store, transmit, and retrieve information, we focus on a subset of information security that is to say on the security of information systems that are based on information technology. We now call an IT based information system "ITIM", in case of more than one IT based information systems we name them "ITIMs", and we refer to the security of IT based information system as "SITIM" and "SITIMs" respectively.

2.1.1.3 COMPLIANCE WITH LAWS

The augmented use of business integrated electronic information systems leads to an increased requirement for high quality IT services. IT organizations are being tasked with establishing mechanisms for more effective, systematic control of fundamental business processes. Leveraging IT to enhance business processes with transactional transparency is also a necessary response to corporate governance scandals[42]. There are several regulatory issues and legislation an organization has to adhere to. Compliance with these rules is becoming a primary concern for almost any organization.

Abbr.	*Legislation*
SOX	Sarbanes-Oxley Act – An act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes[64].
GLBA	The Financial Modernization Act of 1999, also known as the "Gramm-Leach-Bliley Act", or GLB Act, includes provisions to protect consumers' personal financial information held by financial institutions[62].
BASEL II	The "Basel II" framework, or Revised Framework, as the new standard is frequently called, seeks to improve on the existing rules by aligning regulatory capital requirements more closely to the underlying risks that banks face[8].
FISMA	The U.S. Federal Information Security Management Act of 2002 states that "each [Federal] agency shall develop, document, and implement an agency-wide information security program, …, to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source…"[61]
HIPAA	Medical Privacy – U.S. National Standards to Protect the Privacy of Personal Health Information[63]

Table 1: A non exhaustive list of legislations around the world addressing governance

By definition, part of any such program includes proactive system maintenance to protect and ensure information integrity through privacy, confidentiality and access control. For example the SOX 404 attestation requires confidence in the IT systems that house, move, and transform data. This requires confidence in the processes and controls for those IT systems and databases[40]. To address such and other IT concerns IT frameworks were designed.

IT frameworks are generally accepted as best practices. Whether they are government publications such as the Information Technology Infrastructure Library (ITIL), or industry organizations, such as the IT Governance Institute publishing Control Objectives for Information and related Technologies (COBIT), IT frameworks promote quality computing services in the information technology sector.

2.1.1.4 IT SECURITY FRAMEWORKS

Today most of the IT frameworks have sections dealing with security. Whereas some IT frameworks contain guidelines addressing security among other IT concerns other frameworks were just built for IT security purposes. IT security frameworks and IT systems security frameworks respectively can be used to improve the level of security in an organization in a number of ways. They are designed to help organizations keeping the business risks associated with its information systems within acceptable limits. A truly implemented framework is a major tool in improving the quality and efficiency of security controls applied by an organization[31].

Framework	*Description*
CC	The Common Criteria represents the outcome of efforts to develop criteria for evaluation of IT security that are widely useful within the international community. It is an alignment and development of a number of source criteria: the existing European, US and Canadian criteria (ITSEC, TCSEC and CTCPEC respectively)[23].
ISO 17799	ISO/IEC 17799:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management[35].
BSI Grundschutz-Handbuch	The "IT Baseline Protection Manual" contains standard security safeguards, implementation advice and aids for numerous IT configurations which are typically found in IT systems today. The standard security safeguards collected together in the IT Baseline Protection Manual are aimed at a protection requirement which applies to most IT systems[16].
NIST Special Publications	Special Publications in the 800 series present documents of general interest to the computer security community. The Special Publication 800 series was established in 1990 to provide a separate identity for information technology security publications. This Special Publication 800 series reports on ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations[58].

Table 2: A non exhaustive list of IT (systems) security frameworks

2.1.1.5 THE IT SECURITY FRAMEWORK USED

To describe the security process of ITIMs we focus on the NIST framework that provides comprehensive information and tools on this subject. The choice to use the NIST Special Publications as the IT security framework has several reasons. The NIST security guideline is expected to play a key role not only in federal agencies but to have a wide audience beyond the U.S. federal government. The NIST special publications are also closely related to the widely-accepted ISO 17799 IT security framework. ISO 17799 and SP 800-53 are so complementary, that there is even an appendix in SP 800-53 that maps the sections within SP 800-53 back to ISO 17799[59]. Additionally the NIST security guideline provides a risk-based approach which will be very useful in exploring the field of security and prioritizing security measures. Another especially practical point of view is that the NIST series of documents provides explicit guidance - down to the level of specifying base levels of security controls for systems at different levels of risk[22]. And the existence of self-assessment questionnaires makes an audit of IT based information systems much easier for companies.

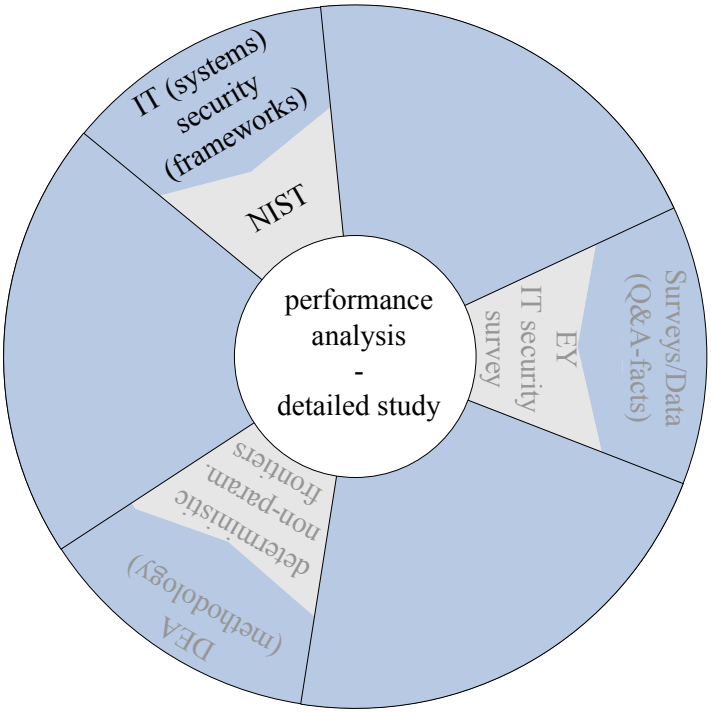

Figure 2: Presupposition one: NIST Special Publications are the specific IT security framework used to analyze performance

2.1.2 DEA METHODOLOGY

DEA is a linear programming based method developed by Charnes, A., W.W. Cooper and E. Rhodes in 1978[21]. It is used to measure the relative performance of processes and organizational units respectively where multiple inputs and outputs make process comparisons difficult. The calculations in DEA are based on the solution of linear programs. This method provides a non-parametric deterministic peer based comparison that can be used to help to identify "star performers and under-achievers". This means that it won't calculate the maximal efficiency that is theoretically possible but the best practices.

DEA can be used with small sample sizes and many such examples can be found in literature[5]. However there is a rule of thumb for selecting an appropriate sampling size. The number of inputs multiplied by the number of outputs will be the number of units assessed as 100% efficient. A large data set and a small number of key inputs and outputs lead to greater discrimination in the analysis of units[29].

Like any other statistical analysis DEA is just an observation tool. It tells you what the sources of inefficiency might be, but it doesn't point out any reason why the unit in question isn't doing well and investigations have to proceed further.

2.1.2.1 ASSUMPTIONS

The efficient frontier consisting of the star performers envelopes (encloses) all other (under-achieving) units (therefore the name "Data Envelopment Analysis"). We have to deal very carefully with this efficient frontier. For one thing noise in the data describing the units could alter the pathway of the efficient frontier. Therefore we assume that the data is free of measurement errors. On another thing there is the possibility that the most efficient unit is outside the sample (e.g. because we don't know of its existence) and is achieving a higher efficiency than the best practice just calculated.

2.1.2.2 OPERATING PRINCIPLES

DEA proceeds on the assumption that the analyzed process is a production process transforming input into output. In general we model inputs as "less is better" and outputs as "more is better". So far it is assumed that the output should be increased and the inputs should be decreased to improve the performance or to reach the best practice frontier.

There are two perspectives on a unit' performance. First we can fix the output while decreasing the input as far as the same output still can be produced. This is called input oriented. The other point of view is to fix the input and to try to increase the output with still

the same resources as input. So we can look for the most efficient unit by either decreasing input or increasing output.

There are processes with undesirable (bad) input or undesirable (bad) output. As far as possible one should go with the positive view, not the undesirable view, i.e. we should use customer satisfaction instead of customer complaints. Apart from the mechanics of the analysis, from a management point of view it is much better to get your staff to work on "customer satisfaction" (a positive thing), than focusing on customer dissatisfaction.

If an increase in the value of an input results in a decrease in any output value we are talking about a bad input. If there is no feasible substitute we model bad input by taking the inverse of the values of that input[11]. In the case a bad output has no surrogate parameter we have two options to design the undesirable. We either use the inverse or we take a large number minus the data values (or a “slightly larger than the largest value” minus the data values) so we don’t get zeros[14].

Some of the inputs are not controllable, e.g. the amount of competitors within a certain distance selling the same items or services. In practice we can use DEA models which can take uncontrollable factors as input.

2.1.2.3 ANALYSIS ISSUES

Finally the scale of operation of an entity can impact the efficiency. Usually an increase in inputs results in a proportionate increase in outputs. But there are circumstances where this assumption is not applicable. For example we have to install a totally new machine to additionally produce a small amount because the existing apparatus is working to capacity. The investment to manufacture this extra small amount is above average and is disproportional. In other words an entity that is efficient compared to entities of identical (or similar) scale sizes can be less efficient compared to entities of different scale sizes. This would mean that the entity under observation is not operating at the optimal scale size. In this case the impact of scale size cannot be ignored. DEA offers tools to probe if the scale size is of importance. The BCC model tells us the efficiency of a unit compared to units of similar scale sizes. That is called the technical efficiency. We auxiliary use the CCR model to determine the efficiency of a unit compared to all units, in particular to units operating at different scale sizes. The efficiency we obtain from the CCR model is identified as the aggregate efficiency. We then compare the results from the CCR model to the ones from the BCC model to find out if the efficiency is scale size dependent.

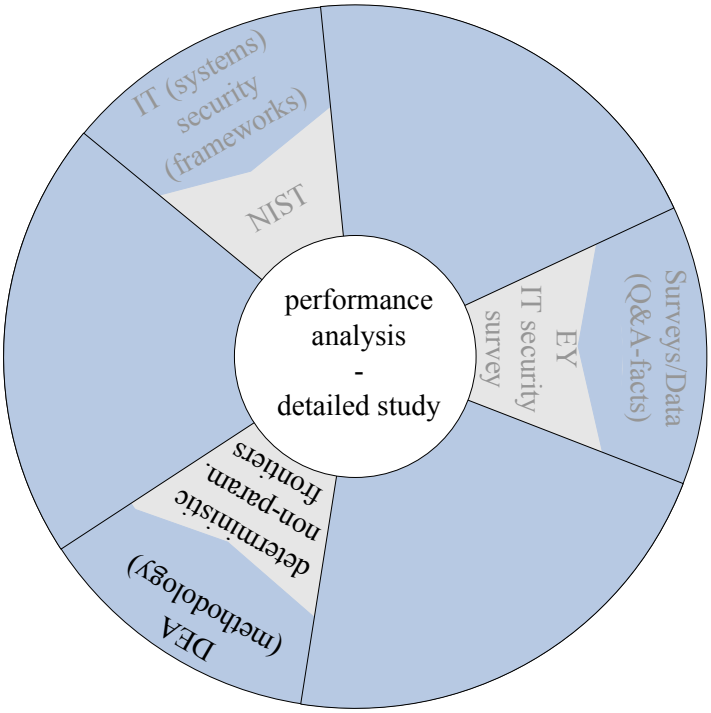

Figure 3: Presupposition two: The kind of DEA models considered for the performance analysis

2.1.3 DATA / IT SECURITY SURVEY

To effectively analyze the real processes we need real world data to answer the questions we want to ask. A survey tells us the current situation delivering up-to-date data. All the big audit firms like Ernst & Young, Deloitte Touche Tohmatsu, PricewaterhouseCoopers, KPMG, conducted their IT security surveys, each with different views and questionnaires on the subject but with similar results. Our study will be carried out using data from the Ernst & Young IT security survey, primary because this information is readily accessible to the author.

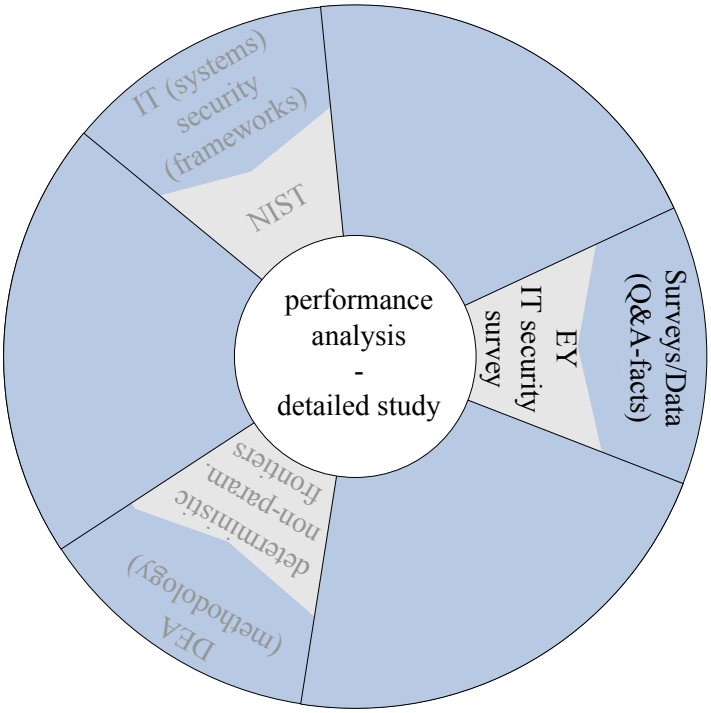

Figure 4: Presupposition three: The specific IT security survey used for the performance analysis

2.2 THE ANALYSIS STRATEGY

2.2.1 THE STRATEGY

The evaluation process and the line of action respectively consist of three phases. First we start from the base of the three pillars we described in the approach section. In the initial phase called concept process we develop DEA models of the security process of IT based information systems. As the models are built we then perform the calculation. This is the application process. The last step is the discussion. There we analyze and interpret the results and draw conclusions about the best practices to secure IT based information systems.

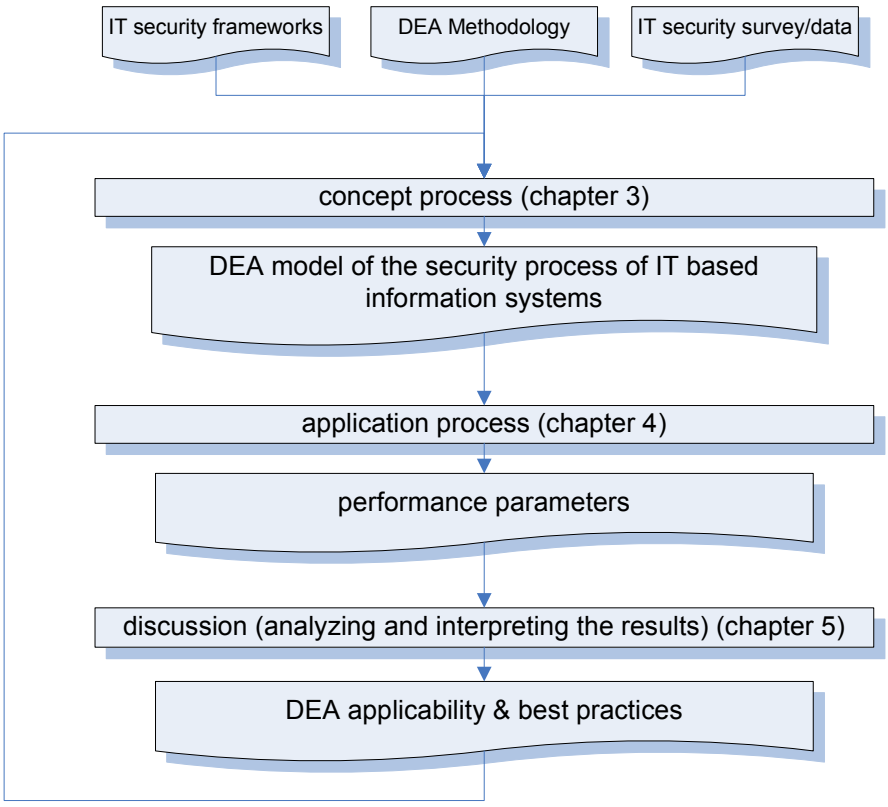

Figure 5: The analysis strategy

As with every more complex project we won't go through this sequence once only. It's a repeating process to continuously improve the know-how of best practices.

2.2.2 CONCEPT PROCESS

2.2.2.1 GOAL

A model of the security process of ITIMs is an abstraction of the real security process. The ultimate goal is to synthesize a DEA model that helps us identifying best practices.

2.2.2.2 ALIGNMENT OF THE ITIM SECURITY MODEL AND DEA

In a first step we create an abstraction of the security process. We then refine the model or models and select the most important inputs and outputs of the security process. These different factors are now to be modeled by means of DEA. Thus we decide how each input and output is represented in DEA. In the resulting constructs we have aligned the security process abstractions and DEA and call them the basic models.

2.2.2.3 ADAPTING THE BASIC MODEL TO THE DATA

We now need data to compute the models. The next task is to check which question of the surveys cover which aspects of the basic models. In other words we search for questions and

their answers respectively that characterize the inputs and outputs chosen. Possibly we have to redefine or simplify the basic model because the questionnaires do not capture all inputs and outputs used. The so formed security process representations are branded as the empirical models.

2.2.2.4 MAPPING DATA TO DEA

Lastly the empirical models will be filled with real data in a manner that they can be computed by means of DEA. Mostly we just create spreadsheets containing the measurements for each input and output of all units under inspection. We refer to the spreadsheets as the implementation.

2.2.3 APPLICATION PROCESS

The efficiencies are now computed based on the spreadsheets. We vary the calculation using two different aspects: input minimization or output maximization and variable or constant return to scale (BCC or CCR). Altering the return to scale model helps us to identify if the size of the units is vital to operate efficiently.

2.2.4 DISCUSSION

Is DEA really applicable to the security process in the field of IT based information systems? This is one of the questions we are going to ask. Another subject is the classification of the behavior of units in respect to their size of operation. Does the efficiency depend on the scale size? Also important are the issues around the main sources of inefficiency and the best practices respectively. Is it possible to identify some mechanisms and to provide advises to improve the level of security in an organization?

3 CONCEPT PROCESS

3.1 THE BASIC MODEL: ALIGNMENT OF THE SECURITY MODEL OF IT BASED INFORMATION SYSTEMS AND DEA

3.1.1 THE SECURITY PROCESS OF IT BASED INFORMATION SYSTEMS

Information security and the security of IT based information systems are much more than a series of technical issues. If done correctly, security becomes a key component of running an effective business[30]. As with quality, the benefit of security is difficult to quantify because the measure of its success is the absence of failure. And as with quality, security doesn't become important until the company recognizes that it's more effective to address problems before rather than after an incident[15].

Although several IT security frameworks and best practices exist, this attitude of inattention might be a reason why there is so few analysis of the security process itself present. There is hardly anything that explicitly describes the security process in a structured manner. Hence the next step is to create a security process model. Additionally we introduce a new factor into risk management. This factor describes to what extend the security of ITIMs supports the business strategy.

3.1.1.1 CONTEXT DESCRIPTION OF AN IT BASED INFORMATION SYSTEM

i) The Environment

Everyone in the information technology industry is aware that information security is important. In every trade or technology-related magazine you will find something about security products. It’s so product-centric everywhere that people are going to believe that you will just “get secure” by buying and using security articles. But security is not a product that you can buy and install. Security is about people, processes, technology and the environment you live in[37].

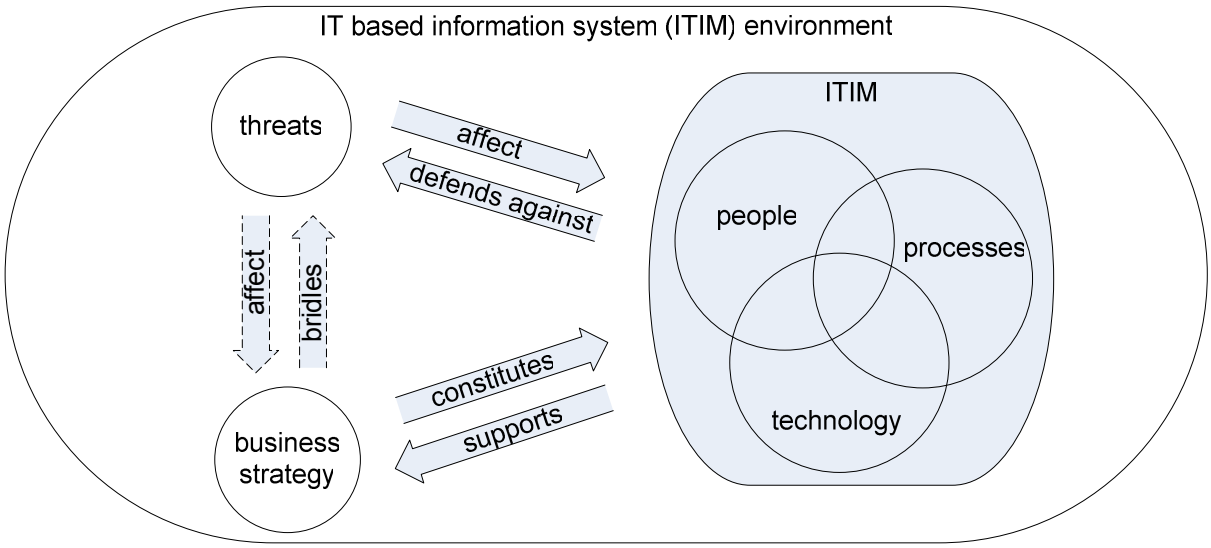

Figure 6: The IT based information system (ITIM) environment

ii) ITIM

The primary objective of an IT based information system (ITIM) is to process and store business information. An ITIM is not only supporting the business processes but is at the same time part of them. First an ITIM consists of the business processes it supports. Secondly it handles the information electronically and automates business processes by means of information technology. Thirdly people participate in the business processes and thus they play a role in IT supported business processes. The ITIM is the entire infrastructure consisting of the implemented business processes, information technology components, and personnel for the collection, processing, storage, transmission, display, dissemination, and disposition of information[60].

Usually there is more than one ITIM. The NIST SP 800-18 further makes a distinction between major applications and general support systems. Major applications are systems that perform clearly defined functions for which there are readily identifiable security considerations and needs (e.g., an electronic funds transfer system). Whereas a general support system normally provides support for a variety of users and/or applications and can be a basis for major applications[48].

iii) Business Strategy

The business strategy is the specification of an organization's objectives and philosophy and its plans to achieve these objectives. The objectives and philosophy are a company's vision and mission that provide high-level guideposts for general decision making. It tells where the business is heading to. The strategic plan describes what is to be achieved, when, and how the firm will move in that direction. The vision, mission, and strategic plan provide a framework

to help managers and employees operate efficiently and in alignment with the company's desired direction[27]. The business strategy is the originator of an information system and the business is the motivation to build ITIMs that in turn support the business and the business strategy.

iv) Threats

A threat is a possible event or occurrence that emerges within a certain probability per period of time and that has the potential to compromise the security of a system or asset[26]. The impact of an actualized threat can not only result in the loss of security but can affect the business mission too. This may include damage to reputation, failure to carry out actions or even worse the inability to complete the mission.

Every threat is raised by one or more sources. These threat sources could perform the action that is menacing us. The common threat sources that have the potential to harm are of natural, human, or environmental kind. In particular humans can act intentionally or unintentionally, by negligence and errors. For example, incorrect travel information to a client that could lead to significant inconvenience is provided inadvertently or maliciously. Threat sources are internally as well as externally. They range from legitimate clients and insiders to criminal organizations and hostile outsiders[17].

Generally details on natural threats sources such as storms and earthquakes are easily available. More and more as intrusion detection tools get popular the quality of the gathered data is improving. Thus the assessment of threat sources and threats is becoming more realistic. The better you know the why and how of attacks the better you can guard your information and assets. As Lance Spitzner[41] says: "… that to understand your threats and to effectively protect against them, you have to understand the bad guys …"[68].

v) Security Objectives

In either case if humans are the source of threats or not, the principal goal of securing the ITIMs should be to protect the organization and its ability to perform its mission, not just its IT assets[51]. The security of IT based information systems protect ITIMs and their information from a wide range of threats in order to ensure business continuity, minimize business damage and maximize return on investments and business opportunities[33].

3.1.1.2 SECURING AN ITIM – A BASIC VIEW

i) Security is a Process

Security indeed is a concern of hardly every part of the business, from core operations to customer relationships. Security is like quality. You cannot buy it, it is not a product. It is a

mindset and a never-ending process[2]. As a result security must be taken as a business process and not as a set of technical instruments.

Most organizations fail to address the numerous security concerns in the field of IT. They see security just as a goal that could be achieved by implementing security tools. Because the securing of IT based information systems is not seen as process most security controls are not implemented with the full understanding of the business. In fact this behavior often leads to an IT security infrastructure that doesn't meet the business needs.

Using a well structured security process it is easier to understand how security measures protect and influence the business. Consequently those responsible can make informed judgments and investments. Our security approach begins and ends with the business and its IT based information systems (ITIMs). We now take an ITIM respecting its business context, have a close look at the threat the ITIM faces and convert the ITIM with the aid of factors of production such as knowledge, manpower, money and technology. The outcome is a reasonable safe ITIM that still fits into the business. The security measures taken and the accepted residual risks are in balance and straightened against the business strategy. Risks are threats weighted in relation to the business[a]. Residual risks are the danger that is consciously not addressed by the company and thus are the potential loss the organization is willing to live with. Closing the security process transforms an ITIM into a risk adequate secured ITIM that is consistent with the defined business strategy and within accepted risks.

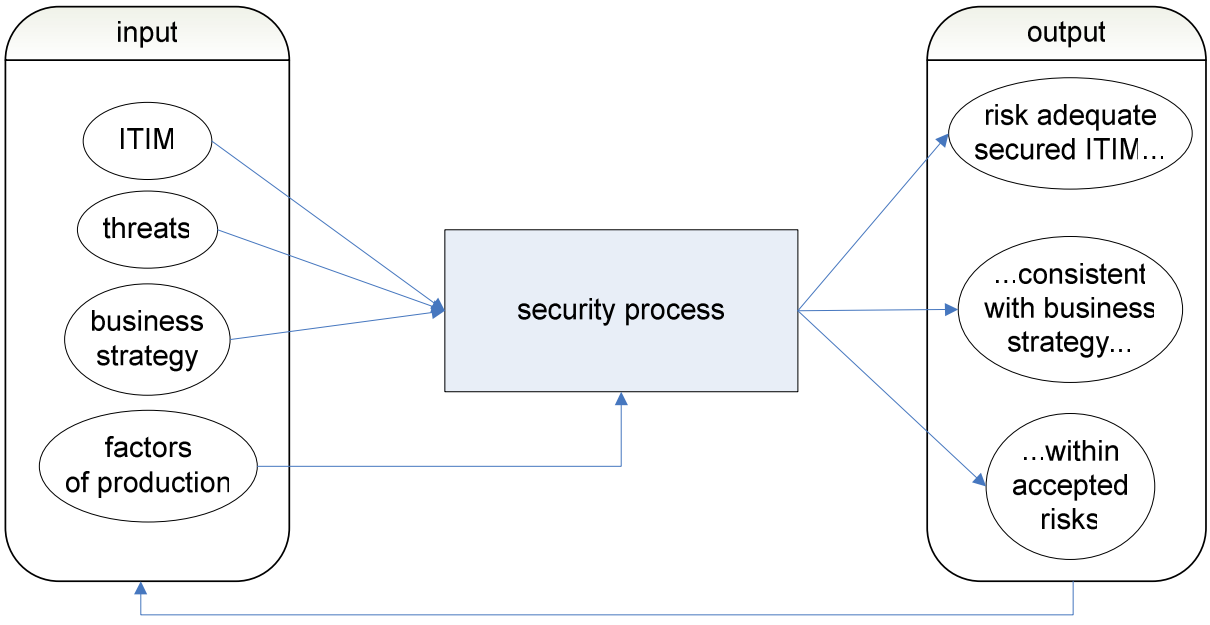

Figure 7: The security process as a transformation process

[a] More on the rating of threats and the exposed risks later in the chapter "The Security Process – The Risk View"

ii) Input

An input is any resource used by a process to produce its output. What do we need to start the security process? What are the inputs of the process of producing security?

First of all, what needs to be protected? We are going to make an ITIM safe, thus the ITIM itself is an input to the security process. An ITIM is made up of three core factors. The people directly working with the electronic information system, the business processes implemented by IT and the IT infrastructure itself. The question we are tackled with is how much ITIM we have to secure. Right now it doesn't interest us how good we have to guard the ITIM. We are just questioning the quantity of the ITIM: The three core factors an ITIM is based on are a good starting point for evaluating the size. As a measurement we could take the amount of persons producing and consuming information by means of the ITIM. Or we could count how many business processes the system implements. Surely there must be a methodology to characterize the integrated business processes and to get a common denominator of what should be numbered. Another way to rate the extent of an ITIM is to have a look at its underlying IT infrastructure. How many personal computers, servers or applications do we have to defend? The resulting measurement of the quantity of an ITIM could be typified by one of the said recordings or by a combination of them and used as the input.

Next we are going to ask what is threatening us. To operate an IT based information system, managers and users need to know the threats. To have knowledge of the surrounding threats and their sources is a premise to deal with them. As input to our security process we do need a list of threats and their sources, supplemented with the motivation of a threat source to realize a certain threat[51]. The identification of that includes the characterization of the threats in respect to the likelihood of their occurrence and their potential impact and now we can quantify the threat factor[b].

As a further important factor the business strategy itself is very difficult or hardly impossible to quantify. But the threats that affect the ITIM indirectly threaten the business strategy too. Thus threats and their materializations respectively have an impact on the ITIM as well as on the business strategy. As we will see later[c] we respect this fact by weighting the threats accordingly. The business strategy and its critical success factors are going to be incorporated as a threat quantifier.

Producing security needs resources: people build up a secure environment, teachers who train awareness must be paid, the budget allows them to buy security products, and so forth. As

[b] See chapter „The Security Process – The Risk View" for more on threat and impact quantification

[c] See chapter „The Security Process – The Risk View"

important as the money available and the amount of employees is the qualification of the coworkers. The quantity of the factors of production that help implement security could be measured e.g. by the IT security budget or a combination of the amount of employees and their qualification.

iii) Potential Attack Surface

We have seen the inputs that flow into the security process, inter alia threats that could endanger an IT based information system (ITIM). But what exactly is exposed that makes an ITIM vulnerable, what of an ITIM is actually threatened, what is the "attack surface"?

The NSTISSC defines information systems security (INFOSEC) as the "Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats"[60]. As we see, in information system, either IT based or not, the object we finally attempt to protect is information itself. In literature the key elements of information security typically identified are availability, integrity and confidentiality[34]. This is not a complete list of aspects of information. There are other aspects too whose contravention could induce security breaches. Further important properties of information are non-repudiation and authenticity. Providentially integrity as defined in the United States Code [44 U.S.C., Sec.3542][65] implicitly addresses these two properties. Using this characterization extends the meaning of the three key elements of information security.

Thus the term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide (A) integrity, including ensuring information non-repudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means avoiding degradation and denial of service attacks[65].

Consequently a loss of *confidentiality* is the unauthorized disclosure of information, a loss of *integrity* is the unauthorized modification or destruction of information and a loss of *availability* is the disruption of access to or use of information or an information system[39]. Confidentiality, integrity and availability as previously declared are the three widely accepted attributes of information and information systems respectively that are vulnerable and the security process must protect an IT based information system from getting these attributes compromised.

iv) Output

An output is any product or service produced by a unit or a measure of how effectively a process has achieved its goals[11].

One target is to get the ITIM secured. Two fundamental issues must be considered on that. First, there is no absolute security. That means no system can be secured by one hundred percent. The second more important issue are the costs involved.

How much does security cost? Are the man-hours used and capital expenditure spent reasonable? Or could we stand some disruption before we have to take action[18]? Can we live with some potential losses? Do we really have to protect against every threat? Sometimes we are even not able to set up enough protection because of the lack of resources and the given timelines. Consequently, mostly we have to tolerate some potential losses. As an output, there should be a report listing the accepted potential losses. The security process[d] provides a defense planning sub-process that quantifies these accepted potential losses in the form of residual or accepted risks. Basically we want to have as less potential losses as possible. So principally the accepted risk is an undesirable output and we call it a bad one.

We must protect the ITIM from the not accepted potential losses. But how do we measure the realized protection? It is an elusive issue that we want to evaluate, mainly because the success of the defense is indicated by the absence of failure and absence of effective attacks respectively. Hence we try to bypass the direct measurement and look for a surrogate variable describing protection. There are two topics that concretely characterize protection: these are the implemented security controls and the presence of successful assaults. The former is the realized guard of an ITIM and as such a positive aspect; the latter tells us about the failure of the defense and as such is an undesirable happening. Therefore the secureness of an ITIM is expressed by these two elements.

Security controls are the management, operational, and technical safeguards that protect the confidentiality, integrity, and availability of an ITIM and its information. We can measure the effective implementation of the utilized security controls. The NIST special publication SP 800-55[55] offers guidance on how an organization can develop and implement a metric framework. Based on this assistance we identify the progress of implementation of the security controls. In addition NIST SP 800-53 provides a comprehensive list of security controls that satisfy the breadth and depth of security requirements. All the security controls in SP 800-53 should be addressed and implemented according to the risk level[53]. Now, taking

[d] See chapter „The Security Process – The Process View“

the metrics framework and the recommended security controls together, we can measure the effectiveness and implementation progress of security controls by means of the SP 800-26 self-assessment guide[49]. The resulting report quantifies the implementation progress. Because we strive for the maturity of the security control realization the implementation progress principally is a positive output.

Sometimes the ITIM has not been adequately secured and we get negative security-related incidents that should have been avoidable[12]. This may be due to a not accurately implemented security control or because a security control does not adequately address the given threat. The harm we get can be differentiated in three components. First there is some immediate ITIM infrastructure damage. That causes certain reproduction costs to restore the ITIM to a secure state. Most of the time, a security event provokes the outage of business services too. Here additional costs arise. For example an E-Commerce Website that is broken down prevents the customer from placing orders during downtime. Finally there are indirect business costs following the security incident beyond the ITIM restoration, e.g. a loss of reputation and the effort to raise one's reputation respectively. We can measure security breaches using the amount of money we lost or counting the number of negative security-related incidents. Since the more breakthroughs we have the worse it is, we principally state that this output is a negative one.

The other objective is to ensure that the ITIM is still in shape with the business strategy. It is not adequate to only protect the ITIM. Do the security controls make the business more difficult or do they even hinder commercial activity? Or do they proactively assist the business strategy? A secured ITIM is still part of the business processes and therefore should fit into the entire company' picture. The installed security controls and their consequences respectively should be in a well founded balance with the success factors. For example a customer centric strategy is envisioned. For customer's safety the client communication is encrypted best but it is unusable because the customer's procedure to establish the communication is far beyond any reasonable expenditure. In another case every business unit's information system is considered per se and gets perfect network protection by means of firewalls, isolating the units from each other. But one of the competitive advantages and success factor is the easy flow of information between the different business units. One more illustration is a company whose strategy is to grow through acquisitions. Although the firm's ITIMs are secured as needed, the IT infrastructure is not flexible enough to support the growth strategy because the security measures lock the ITIMs. In the end it depends on the business strategy to what we are going to have a closer look at and what subject we are going

to investigate further. A possible approach to get a current picture is to conduct an inquiry based on the business strategy and thus on the success factors. The report then tells us how well security measures have had supported these success factors. Another proceeding is to interview employees and customers to learn more about the benefits and barriers IT security arrangements place. Then these results will be adjusted to the success factors. A combination of all these facts states how effectively the business strategy has been supported and implemented by the SITIM; it describes the business strategy alignment output. Basically we want to support the business strategy. Thus the business strategy alignment is principally a positive fact and hence a good output.

v) Mode of Action – Fundamentals

We identified the resources and objectives of the security process. We know now what the inputs are and what outputs the security process produces. At the moment the security process itself is just a black box. And we want to keep the complex relationships hidden in the box. But we are interested in how changes in the input basically influence the outcome. Does an input contribute to the outputs or is it an undesirable input lessening one or more output? Although the details of the securing function don't concern us we want to know the fundamental rules and thus the mode of action of the inputs.

Usually for a production process we principally assume that the more resources we have the more output we should get. This is true e.g. for a bakery; the more flour they take the more bread and croissants we can buy. We don't state anything about the quantity. For example we don't say with the doubled volume of flour the baker produces the double amount of croissants. But we know that flour is in positive correlation with any output and thus declare this input as a good one.

How do the efforts in the field of security relate to the production? We now complete the basic description of our security process by making the mode of action explicit. We define three fundamental rules. These axioms cover each input except the business strategy that indirectly flows into the process via the threats:

(1) The more threats we have, the more protection is needed.
Basically more threats imply less protection, fewer threats imply more protection; thus the amount of threats is principally an undesirable or bad input.

(2) The larger the ITIM is, the more the demanded protection is.
That is because a larger ITIM exposes a larger surface that faces the threats.
Basically a larger ITIM implies less protection, a smaller ITIM implies more

protection; thus from a security point of view the largeness of a system is principally an undesirable input.

(3) The more factors of production we have, the better protection we get.
Basically more security resources such as manpower, money, and so forth imply better protection, less security resources imply less protection; thus the factor of production is principally a positive factor and hence the amount used a good input.

3.1.1.3 THE SECURITY PROCESS – THE PROCESS VIEW

Let us have a closer look at the security process itself. We know what we are going to protect and what issues we have to take into account; and we have got a concrete idea of the output. What remains to be explained are the steps to secure an ITIM. What is happening in the black box?

i) The Security Process

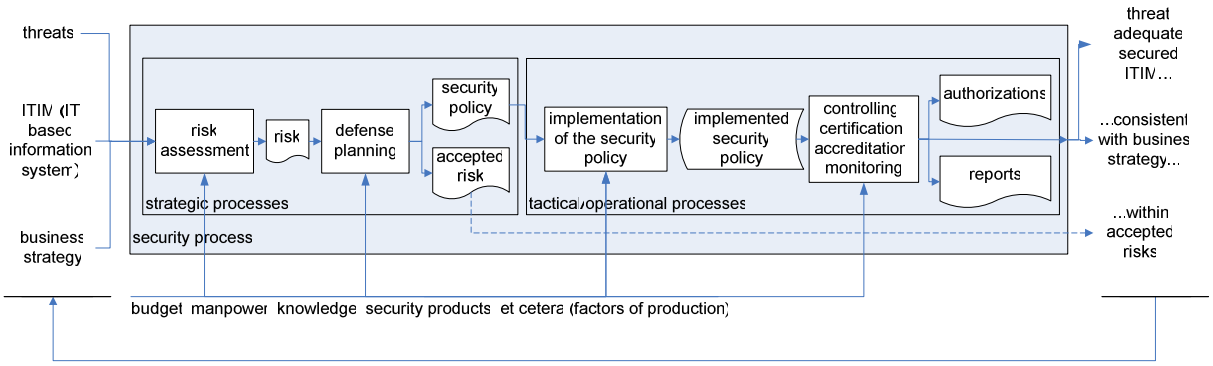

Figure 8: The detailed security process.

First we collect information about the environment and work it up. We gather details about the IT based information system we are going to secure, we collect data about the threats, and we analyze the business strategy. We ask us what needs to be protected, why it needs protection, and how it is threatened[20]. In the risk assessment process we quantify and thus prioritize the threats. The result is a snapshot of the current danger and we call it the risk we are facing.

With the help of this picture of the current security-related situation we then can decide on the action that must be taken. The goal of the defense planning is a plan to protect the organization's ability to perform its mission, not just its IT assets. Carrying out this process we ask how to avoid and prevent potential damage[28]. In some cases, we may find it more cost-effective to simply tolerate the expected losses[47]. The result we further use is the security policy that contains the description of the security controls we are going to install. The

security policy is the plan saying how to reduce risk to an acceptable level and maintain that level of risk.

Until now we actually haven't implemented protection. We have just thought about it and identified the necessary preparations. Overall, the character of the processes that finally deliver the security policy is more of a strategic one. The security policy is an important milestone and this plan prepares us for the security implementation.

With the security policy the management determines the best course of action. Now we implement the security controls just like they are defined in the security policy. These safeguards address different aspects, e.g. how to protect the physical infrastructure, how to identify and authorize users, how to train employees and raise security awareness, and so forth.

The next step is to control the implementation progress and to demonstrate the effectiveness of the safeguards. We determine the extent to which the security controls in the ITIM are implemented correctly and operating as intended. The outcome will be certified in respect to the system's security requirements and to the security policy respectively. Based on this security certification the authorizing officials will have the information needed to decide on the ITIM's accreditation to operate. Throughout the life cycle of the ITIM we continuously have to oversee and monitor the ITIM and its security controls and identify changes whose result could impact security. Reports on alteration to the system or its operational environment and information about the system state will be communicated with the corresponding persons in charge.

Now we have effectively built the safeguards defined in the security policy. Controlling and monitoring are the day-to-day operations we conduct on the current ITIM and on its actual security controls. The constructing, controlling and monitoring are the tactical and operational processes.

Closing, the mission and business process, the threat situation and the ITIM change over time. Because these inputs vary the security requirements and protection methods must be updated. Thus the security process is ongoing and must be performed periodically[50].

ii) Measuring the Security Policy

The security policy is the product of the strategic processes and the base for the security implementation. To characterize the quantity of the security policy we measure its coverage. We have to do this within a defined framework. The Computer Security Division (CRD) provides such a framework we can measure against. This framework is the NIST special publication SP 800-53. It is a comprehensive list of security controls and we define that these

controls are the target controls that have to be addressed. In practice we would use the SP 800-26 questionnaire that is based on the special publication SP 800-53. We now compare the current security controls brought up in the security policy to the target controls and count the matches. This results in the amount of the actually addressed controls in respect to the target set. This current amount divided by the amount of security controls of the target set of SP 800-53 or SP 800-26 gives us the degree of the coverage of a security policy and thus the quantity.

iii) NIST Security Framework Integration

The security process we described contains the two main processes risk management consists of: risk assessment and risk mitigation. These basic risk management activities should always be performed irrespectively of what kind of risk management model one chooses[47].

Risk assessment is the process of analyzing and interpreting risk. This is consistent with our risk assessment process whose result indicates the endangerment of the system or asset. NIST supports this evaluation with the guidelines FIPS 199[45] and SP 800-60[56]. These documents help defining the category of information systems according to potential impact of loss[32]. The risk assessment is used to sustain two related functions of the following risk mitigation process: the acceptance of risk and the selection of cost-effective controls.

Risk mitigation is the process of security control selection, accepting residual risks, implementing the chosen safeguards and monitoring the effectiveness of implementation[43]. The risk mitigation process corresponds to our last three processes whereas the selection of security controls matches with the defense planning process which also supplies the accepted risks. Security controls are the management, operational and technical safeguards and countermeasures for an information system. FIPS 200[46] defines the minimum security requirements and NIST SP 800-53[53] assists in deciding on security controls. Using well-written, standardized checklists to configure products, as specified in NIST 800-70[57], can markedly reduce the vulnerability exposure of IT products. After the implementation NIST SP 800-53A[54] facilitates the assessment of the effectiveness of security controls employed in information systems. NIST SP 800-37[52] helps certifying the fulfillment of the security demands in order to issue authorizations to operate.

A foundation for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems, is made available by NIST SP 800-30[51]. It generally supports our risk approach to security. The entire security process and thus the protection of a system must be documented in a system security plan as delineated in NIST SP 800-18[48].

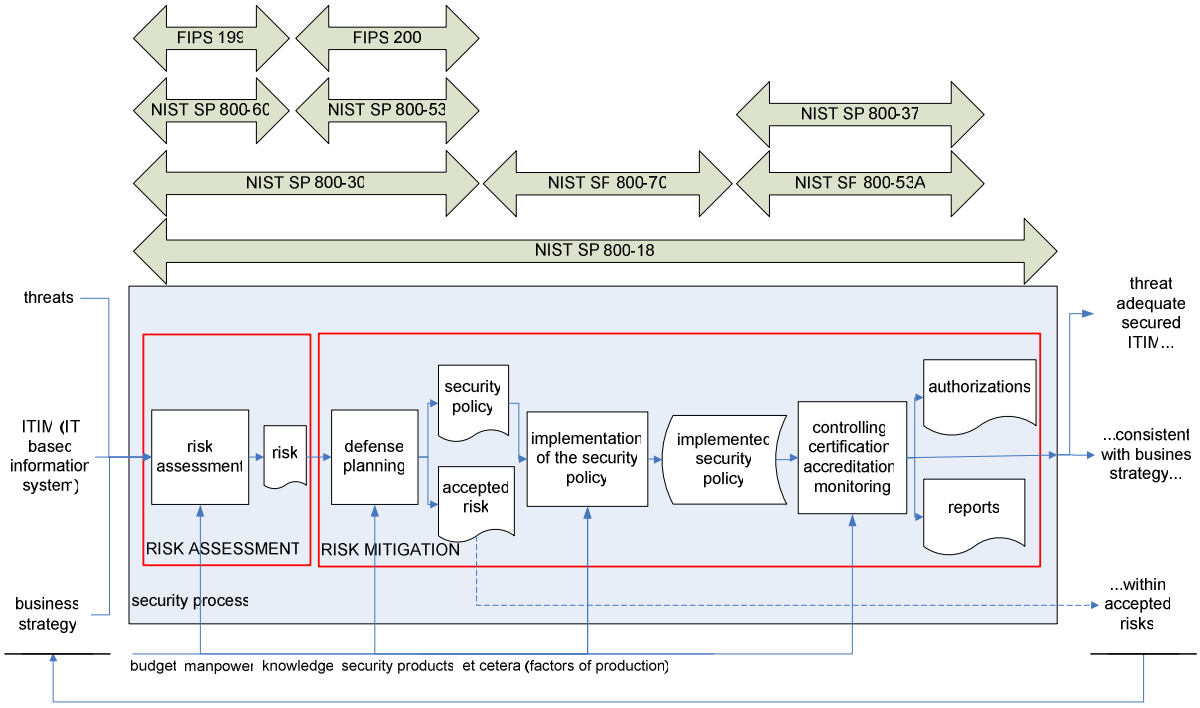

Figure 9: The integration of NIST' security management framework

3.1.1.4 THE SECURITY PROCESS – THE RISK VIEW

Managing security is an enterprise wide task. The specification and implementation of security controls for an ITIM is part of a security program that manages risk across the entire company. The risk-based approach to security enables the management to prioritize security undertakings and to make well-informed risk decisions. A risk assessment that explicitly supports the business strategy ensures the appropriate selection and specification of security controls.

i) <u>The Threats</u>

The threats are the reason why we principally have to protect assets. A threat occurs within a certain probability per period of time. Generally the forecast for natural disasters is more accurately than predicting malicious intention. In addition a threat, e.g. the theft of my bike, can root in more than one threat source, e.g. it could be stolen by a criminal organization or by someone who just didn't want to walk home. Usually the more sources a threat has the more likely it is that the undesirable will happen.

Moreover a threat inherently has an objective it intends to impact. For ITIMs a threat is targeting the confidentiality, integrity, and/or availability of the system. We further could classify threats by the part of the system they are attacking; namely if the people, processes or technology of an ITIM is assaulted.

A threat that has occurred does not only impact the confidentiality, integrity, and/or availability of a system and thus the business. Most of the time the threat transforms an ITIM to an unsecured state or it even destroys the infrastructure. Hence a threat can affect the business as well as the ITIM itself. We distinguish between the reproductions costs of an ITIM, the direct business costs that instantly arise, and the indirect business costs that follow the negative security event in the long run.

After a security incident we probably must repair the ITIM and get it into a secured state. The costs associated with this reconstitution are called the reproduction costs. Next the business is almost certainly directly affected by a loss of confidentiality, integrity, and/or availability of the ITIM(s). For example before the court the evidence couldn't be supplied because of the loss of authenticity of this electronic evidence. Or in case an E-Commerce site has been broken down the lost availability results in a financial minus and this lost productivity can easily be calculated, e.g. using the average orders placed per period of time multiplied the average value of the purchase. Business expenditures directly related to the harmful happening are defined as the direct business costs. Sometimes the impact of an undesirable occurrence is widespread and it influences the business late beyond. For example the fact that credit card numbers are stolen causes damage to the firm's reputation. Businesses costs that come up after the restoring of the ITIM are called indirect business costs. Generally the indirect businesses costs are characterized by the fact that they are hardly to estimate and mostly their value is just guessed. The total impact of a threat is determined by summing up the reproduction costs, the direct business costs, and the indirect business costs.

$$\text{impact}(\mathit{threat}_i) = \begin{pmatrix} \text{reproduction\_costs}(\mathit{therat}_i) \\ + \text{direct\_business\_costs}(\mathit{therat}_i) \\ + \text{indirect\_business\_costs}(\mathit{therat}_i) \end{pmatrix}$$

Formula 1: Calculation of the impact of a certain threat

ii) The Business Strategy Aspect

An organization must perform well in certain key areas to achieve its mission. These key areas can be defined as the organization's critical success factors. In the long run the effectiveness of protection depends on how well the security controls are aligned with and support the organization's business strategy and its critical success factors[20]. So, from the beginning, we must consider the importance of an ITIM in respect to the firm's critical success factors. The business relevance of the confidentiality, integrity and availability of an ITIM will be part of the estimation of the ITIM's endangerment.

The business criticality of an ITIM is measured by weighting the confidentiality, integrity and availability. We assign a value to each property to represent the importance for the business and mark them with low, moderate, and high. Then the business criticality of an ITIM is the highest value given to any of the three topics.

$$\text{business\_criticality}(ITIM_j) = \max \begin{pmatrix} \text{value}(confidentiality_j) \\ \text{value}(integrity_j) \\ \text{value}(availability_j) \end{pmatrix}$$

Formula 2: The calculation of the business criticality of a certain ITIM

In addition the quantification of the importance of the confidentiality, integrity, and availability can improve the communication between the business and the IT unit and serve as a "business people – IT people" interface. The business people have a way to express their security requirements in respect to an ITIM and the IT people can understand this kind of claims and can satisfy them.

iii) Risk Assessment

Through the analysis of threat probabilities, impacts, and the business criticality of an IT based information system we gain an insight into the risk the ITIM is facing. Weighting the threats according to their probability of occurrence, their potential impact and their influence on the business we can prioritize security actions and make well informed protection decisions. The stakeholders can understand the man-hour and capital expenditure requirements and can plan security projects with respect to their situation[19].

The purpose of the risk assessment is to measure the endangerment of a system or asset. With the risk factor we express this hazard. The risk referring a certain threat and ITIM is calculated as the business criticality of the ITIM multiplied the probability the threat event occurs multiplied the impact the threat event can cause. The total risk for an ITIM is measured analogous and calculated as the sum of all single risks.

$$\begin{aligned} \text{risk}(ITIM_j) &= \text{sum}_i \begin{pmatrix} \text{probability}(threat_i) \\ \times \text{impact}(threat_i) \\ \times \text{business\_criticality}(ITIM_j) \end{pmatrix} \\ &= \text{business\_criticality}(ITIM_j) \times \text{sum}_i(\text{probability}(threat_i) \times \text{impact}(threat_i)) \end{aligned}$$

Formula 3: The calculation of the total risk of an ITIM

The classical approach of risk calculation considers the probability and impact of threats. In addition we want to incorporate the business explicitly. Thus we have introduced the business criticality of an ITIM as a further weighting factor. This proceeding provides several advantages.

First, the security planning should concentrate on those threats most likely and affecting important assets. By incorporating the businesses importance of an ITIM into the risk calculation we can better prioritize threats with respect to the business strategy. Thus in the security or defense planning process we can really focus on the protection of assets that are important to the business. This guarantees us an improved understanding of the security needs and mission assurance.

Another very important aspect is the uncertainty you face estimating a threat properties. How often might a negative security-related incident happen? How bad could it be? How sure are the answers to these questions[28]? Sometimes we don't know the reliability of the numbers. Thus in some cases we don't know how realistic certain threats are[47]. Introducing a further factor into the classical risk calculation shifts the weighting. The probability and the impact factor will be less relevant computing the risk. Thus the uncertainty in characterizing the threats' properties is less serious. Accessorily the newly introduced factor brings a real business point of view.

iv) The Individualized Risks

A further advantage of the business criticality factor is the easiness to individualize risk down to the single company. Using the classical risk calculation approach we could differentiate between industries by including and excluding threats and threat sources. Every branch has another environment and hence the threats and threat sources often aren't congruent. For example a bank has to defend against pishing attacks whereas a bakery without an online shop can ignore that threat. So we easily can individualize the risk per industry or sub-industry by defining the corresponding set of threats and threat sources.

Intra industry each company has its own key areas that are its unique success factors helping to compete in that industry. Hence each firm has its own important and critical assets. Addressing each firm's business strategy and critical success factors establishes us to individualize risk referring these custom assets. By using the business criticality factor we have a comfortable method to project the critical success factors onto the risk assessment and thus we could easily individualize the risk per company.

v) Risk Management Assumption

The security process isn't just a point in time. It takes time to analyze the endangerment and to plan and implement security solutions. Threats can change and the business strategy could shift, especially in fast pacing industries. Thus the risks we face during the risk assessment have not to be the same after the protection installation. But for simplicity and the ease of efficiency analysis we state that during the period we study the risks don't change. Parsing the risk formula we mainly see three variables: the probability of threats, the impact of threats, and the business criticality of an ITIM. Thus having stable risks means that the threat environment must not change and the business strategy has to be constant, at least during the period of analysis.

Previously we discussed the influence of threats to the security process. We stated that more threats require more protection and the amount of threats is a bad input. Because the risk is nothing else than somehow weighted threats, it is straight forward to determine that the risk is a bad output too. In literature it would be called a downside risk in contrary to an upside risk which represents a chance.

3.1.2 THE SECURITY PROCESS MODEL - CHOICE OF INPUTS AND OUTPUTS

We describe the security process defining the inputs and outputs. Therefore the choice of these variables is of paramount importance. Thanks to the study we conducted we have now a funded idea of what the inputs and outputs are. The task now is to choose and formally describe the factors that shall represent the security process.

First of all we want to represent the security process as accurately as possible. We are looking for variables that indeed characterize the process. We try to avoid using variables that describe the same. If two variables are highly correlated, they may both represent the same basic data. Thus we would eliminate a variable if we could[4].

3.1.2.1 MODEL ASSUMPTIONS

The following statements about the security process have an effect on the choice of input and output factors.

i) Simplification of the ITIMs Infrastructure

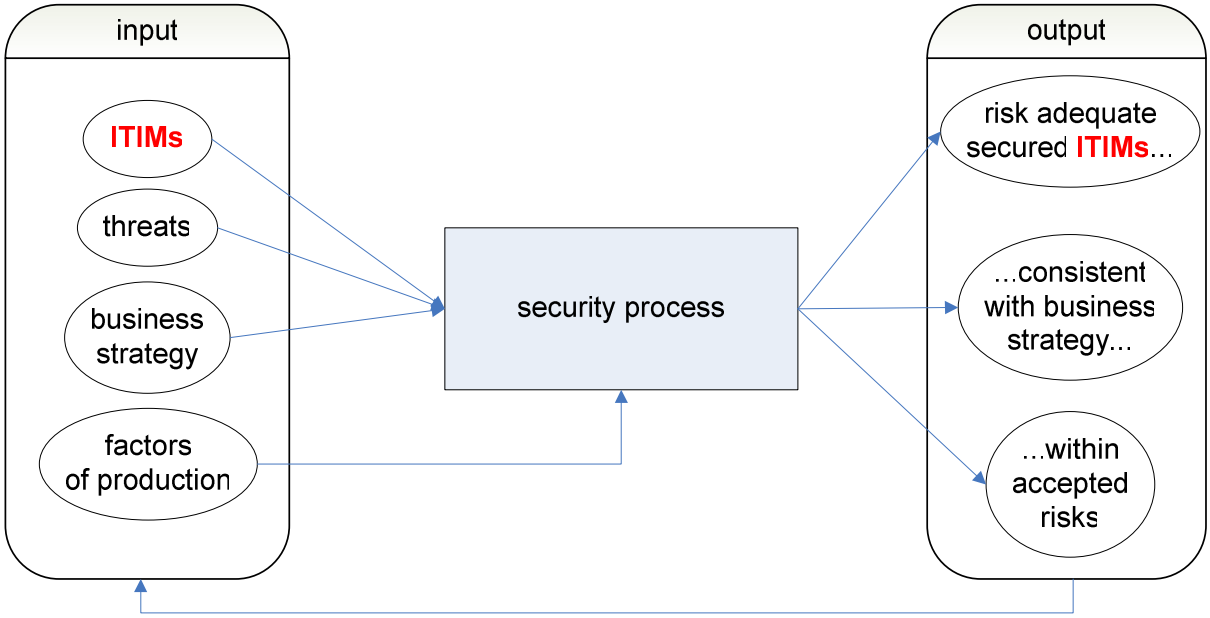

Figure 10: The security process handling more than one ITIM

To begin with an organization has not just one ITIM. Usually there are many more. Some of them are general support systems; some others facilitate specific business processes. Because all these ITIMs belong to the same organization it is reasonable to say that they are located within the same environment. Thus we state that all ITIMs of a company face the same threats and are subject to the same business strategy. Therefore it is reasonable to take all the ITIMs together and view it as one large system. For simplicity and practicability we now treat an organization's ITIMs as one ITIM.

ii) Mode of Action

The most important thing is the view of the functionality of the security process. How does the security process work? What are the roles of the input factors? To do a funded analysis we must make our assumptions explicit; we must clearly state what the input factors effect. The following axioms have been deduced in the previous chapters. For the sake of completeness and comprehensibility we specify them again.

(1) The more risk we have, the more protection is needed.

Basically more risk implies less protection, less risk implies more protection; thus the amount of risk is principally an undesirable or bad input.

(2) The larger the ITIM is, the more the demanded protection is.

That is because a larger ITIM exposes a larger surface that faces the risk.

Basically a larger ITIM implies less protection, a smaller ITIM implies more

protection; thus from a security point of view the largeness of a system is principally an undesirable input.

(3) The more factors of production we have, the better protection we get.
Basically more security resources such as manpower, money, and so forth imply better protection, less security resources imply less protection; thus the factor of production is principally a positive factor and hence the amount used a good input.

iii) Risks

Next we declare that all organizations do business within the same environment. We don't differentiate between industries and we don't consider individual business strategies. This means that the threats, the threat sources and the business strategy are the same for all companies. Consequently the threat probabilities and the business criticality are identical.
Sharing the same business strategy it is reasonable to state that the impact of a certain threat is basically the same and between different organizations this impact only differs proportionally according to the business size:

$$\text{impact}(threat_i, organization_s) = \text{size}(organization_s) \times basic\_impact_i \quad \text{for all i and s}$$

Formula 4: Assumption that a certain impact differs proportionally

Let us take these three assumptions together. We then set the variables of the risk formula accordingly:

$$\text{risk}(ITIM_j) = \text{business\_criticality} \times \text{sum}_i(\text{probability}(threat_i) \times w \times basic\_impact_i)$$
$$= w \times \text{business\_criticaltiy} \times \text{sum}_i(\text{probability}(threat_i) \times basic\_impact_i)$$

for all i, j,
where $w = \text{size}(organization_j)$
and the $ITIM_j$ is the entire ITIM of organization j

Formula 5: Assuming a constant environment, the risk is proportional to the business size

We see that based on the three assumptions made before, the risk of an organization's entire ITIM is proportional to the business size.
Often the size of the company's ITIM corresponds and correlates to the business size. So it's reasonable to associate the business size with the size of the ITIM. Hence the next presupposition is that the risk of the organization's ITIM is proportional to the size of the ITIM.

Consequently the risk and size of the businesses ITIM do positively correlate: both bad factors describe the same. Thus using both input factors doesn't increase the quality of the description of the security process. Eliminating the risk variable reduces the dimensionality of the problem and will increase the discrimination of the analysis. We now proceed without explicitly using the risk factor and the business strategy.

iv) Stable Threat Frequency and Constant Business Objectives

Although we do not explicitly deal with the individual business strategies and threats this doesn't release us from paying attention to these factors. Primarily we are interested in the changes these factors exhibit. As we have seen the security process isn't just a point in time and for a basic analysis we need stability for the period we study. Thus we assume that the threat environment doesn't change and the business strategy is constant during the period of analysis.

v) Accepted Risk

Finally the residual risks or accepted risks are extraordinarily difficult to measure. If there is no structured risk management it is sheer impossible to quantify the not addressed endangerment. It would be very helpful to describe the security process without this output variable.

First the risk strategy of an organization defines how many percent of the risk the organization will accept. Using the same percentage, firms facing more risk will have more absolute risk accepted than companies confronted with less risk. Previously we have defined that the business strategy is identical for all organizations. Consequently they have the same risk strategy and percentage of risk acceptance respectively.

Further we have stated that the risk an ITIM is confronted with will be expressed by the size of the ITIM. Thus, assuming same risk acceptance, the accepted risks are basically the same and between different firms the amount of accepted risks only differs proportionally according to the size of the corresponding ITIM. Now, because the accepted risk and the size of the ITIM are positively correlated and both factors are bad ones and describing the same, we eliminate the accepted risk factor and exclude this output factor from describing the security process.

3.1.2.2 RESOURCE AND COST EFFICIENCY

A factor can be measured differently. For example the manpower used could be expressed by the working hours or the sum of salaries. The working hours reflect the input in a technical manner, whereas the wage bill is the economical point of view. We see there are many facets

of efficiency. We could analyze the efficiency using technical parameters or economical indicators or a combination of both. The main point is to keep in mind how the factors were measured. Mainly we try to get a technical characterization of the factors.

3.1.2.3 FACTORS

The values of the input and output factors are subject to several limitations. First of all the factors must be quantifiable. Further we avoid zero values because they present a problem in ratio performance measurement[3]. In addition the data values must be positive.

i) Input

The inputs associated with the security process have to be classified as either controllable or non-controllable parameters.

The first input is the system size. Sometimes we can slightly reduce the system's extent by removing unnecessary or seldom used computer terminals. But generally we deal with a system of a given size. It does not make a lot of sense to talk about changing or reducing the amount of computer terminals only in respect to security considerations[6]. Hence the system size is an uncontrollable factor. Interfaces, whether physical or logical, are a main characteristic of an ITIM. The personal computers are the key input and output interfaces of an ITIM within a company. Hence it is reasonable to measure the system size by counting all computers used by employees. Previously we identified the largeness of a system as a bad input. Thus the total of all personal computers within a company is an uncontrollable bad input.

The next inputs we are going to include are the factors of production. We differentiate between the staff involved into the security process and other resources used to transform an ITIM. The staff factor will be measured in working hours. All other resources are quantified by the IT security budget minus the personnel costs. The working hours and the adjusted IT security budget are controllable and good inputs.

ii) Output

The key element in the line of defense against threats is the effective implementation of the security controls that are defined in the defense planning process. Now we want to identify the current status of the installation of security controls relative to the existing security policy. This means we want to measure the implementation progress and the effective installation of our defined security controls respectively. Self assessment tools make it easy to systematically gather information and help to determine the current status. The NIST's ASSET[44] (Automated Security Self-Evaluation Tool) is a self-assessment tool that assists gathering data and

automates report generation determining the current status of the security controls. This result will be used to describe the installation progress. From this we calculate the implementation degree that is a positive output.

Negative security-related incidents happen either because threats are not addressed or because the security effort doesn't suffice. For the protection analysis we are only interested in the latter category. This means we just want to measure the negative security events that should have been avoidable. These incidents are breakthroughs sweeping off our line of defense. This could happen because of ineffectively implemented security controls or of safeguards that do not adequately address the corresponding threat. We measure the magnitude of negative security-related incidents by counting the amount of virus outbreaks, the downtime of the ITIM, and so forth. A combination of these quantities indicates the amount of avoidable security breaches and is a negative output. In addition we have to take into account that first of all we have to become aware of an event. Obviously, it is possible that some events may rest undetected. Thus the finding if a system is penetrated depends on the quality of the control process. This uncertainty of detection must be addressed. Therefore we multiply the amount of security breaches by the degree of uncertainty of detecting a security event. This adjusted result is a bad output.

How well are the security measures aligned with the business strategy? Do they interfere with the current success factors such as e.g. facilitating mergers and acquisitions, enabling strategic initiatives, and enhancing customer experience? Best is to start an inquiry asking the different parties specific questions about the security measures to determine the support or hindering to the company's success factors. The result is the degree of business strategy support and a positive output.

Finally the security process generates reports about success and failure. In turn this information about system security is not only an output, it is an important basis for further security actions. Thus the reports and the communication of the system status and the security status are vital to protect an ITIM. The simplest way to characterize this issue is to identify how often reports were communicated to strategic security planners. This communication frequency is a good output.

3.1.2.4 THE SECURITY PROCESS MODEL

We are going to investigate the whole security process and to calculate the overall performance. As the input we take the system size (SYS), indicated by the total of all personal computers, the staff used (STAFF), measured by the working hours, and the remaining factors of production (RPROD), quantified by the adjusted IT security budget. The output consists of

four parts: the implementation degree of the security controls (SECON), the rated avoidable security incidents (RAIN), the support of the business strategy (BSTRATSUPP), and the communication frequency of reports (REP).

(*SECON, RAIN, BSTRATSUPP, REP*) = SecurityProcess(*SYS, STAFF, RPROD*)

Formula 6: Formal description of the security process

3.1.3 THE BASIC MODEL

3.1.3.1 FACTOR DESCRIPTION BY MEANS OF DEA

Let us take our input and output factors. Their categorization as good or bad is based on the mode of action we assumed. Next we rewrite our factors according to the DEA methodology and model bad input and bad output as the inverse.

i) System – Input

In DEA we take the inverse of the system size (SYS) because it is a bad input. The system size itself is quantified by the amount of personal computers located within the company.

SYS_{DEAuc} = (1 / SYS) = (1 / (number of pcs)), "$_{uc}$" stands for "uncontrollable" input.

ii) Manpower – Input

The hours the staff has worked is the manpower input.

$STAFF_{DEA}$ = STAFF = (total working hours)

iii) Budget – Input

All other required resources except the staff are expressed by the IT security budget minus the personnel costs.

$RPROD_{DEA}$ = RPROD = (IT security budget) – (staff costs)

iv) Implementation – Output

The degree of the implementation of the security controls used in the company is calculated by ASSET:

$SECON_{DEA}$ = SECON = implementation_degree(ASSET(*ITIM*))

v) Incidents – Output

We count all negative security-related incidents that should have been avoidable according to the defined security policy and combine the resulting number with the degree of the uncertainty of detecting the security event. Thus the more uncertain we are to notice events the bigger the weighted incident number is and hence the smaller this output is.

$RAIN_{DEA}$ = (1/RAIN) = ((number of avoidable incidents) × (uncertainty of detection))$^{-1}$

vi) Business Strategy Alignment – Ouput

We interview the different parties about the benefits and obstacles of the installed security controls and analyze the inquiries in respect to the success factors. The result is the degree of the support of the business strategy.

$BSTRATSUPP_{DEA}$ = BSTRATSUPP = (degree of the support of the business strategy)

vii) Reporting – Output

Basically security breaches should be reported and information about the system status should be gathered and exchanged. We ask how frequently the staff communicates the ITIM's condition to the strategic management.

REP_{DEA} = REP = (freq. of communication with the strategic management on system status)

3.1.3.2 THE BASIC SECURITY PROCESS MODEL

As we have seen, using DEA we must adapt bad inputs and undesirable outputs. Hence the security process formula in DEA is slightly different.

$$\begin{pmatrix} SECON_{DEA} \\ RAIN_{DEA} \\ BSTRATSUPP_{DEA} \\ REP_{DEA} \end{pmatrix} = \text{SecurityProcess}_{DEA} \begin{pmatrix} SYS_{DEAuc} \\ STAFF_{DEA} \\ RPROD_{DEA} \end{pmatrix}$$

or

$$\begin{pmatrix} SECON \\ 1/RAIN \\ BSTRATSUPP \\ REP \end{pmatrix} = \text{SecurityProcess}_{DEA} \begin{pmatrix} (1/SYS)_{uc} \\ STAFF \\ RPROD \end{pmatrix}$$

Formula 7: Formal description of the security process modeled by means of DEA

The appendix "$_{uc}$" means that the marked input is an uncontrollable factor in DEA.

3.1.3.3 CONCLUSIONS

The fundamental question is if we principally can model the security process by means of DEA. With DEA we can analyze processes that transform inputs to outputs. We have shown that we can describe the security process as a transformation process that produces security. Making some assumption we are able to quantify all required factors. In addition all factors can be expressed in a way that fits DEA. Thus the DEA concepts are applicable to the security process.

Finally let us keep in mind that the mode of action of input factors and the characteristics of the output factors are just reasonable and justified assumptions and already an abstraction of the reality.

3.2 THE EMPIRICAL MODEL: ADAPTING THE BASIC MODEL TO THE DATA

The empirical model is a pragmatic approach to the security process. We are looking for data that describe our input and output factors. The descriptions must yield quantifiable information and should be readily obtainable.

3.2.1 THE SURVEYS

3.2.1.1 STRUCTURE ANALYSIS

The Ernst & Young IT security surveys of the years 2003, 2004, and 2005 have been checked. An analysis of the questions reveals that the structures of the surveys do considerably differ. Partly questions don't exist the following year or new inquiries have been introduced to explore other aspects. Thus we do concentrate on one survey. The questions of the 2003 inquiry characterize our inputs and outputs best. About 20 percent of the information provided can be used to describe the factors. Additionally there are a few questions whose answers could possibly act as explanatory factors.

3.2.1.2 QUESTIONS RELATED TO THE BASIC MODEL

i) Input

The first input is the system size that we characterize by the amount of personal computers (pc's) a company uses. Unfortunately there is no information about the total of utilized pc's. We remember that earlier we stated that it is reasonable to count all pc's the employees use. So if every worker has its own personal computer we can take the number of employees to define the system size. Question number three addresses this issue: "How many employees are in your entire organization?".

Next we want to measure the factors of production such as manpower and the IT security budget. Unfortunately there is no information presented about these subjects. But as a workaround we can state that the sum of the factors of production is proportional to the system size. That doesn't reflect the reality well. However it is somehow reasonable because the bigger the system is the more resources are used to get the ITIM safe. The disadvantage of this approach is that we get two firmly negative correlated input factors. Let us keep this

shortcoming in mind. We are going to address it while building the DEA implementation of the empirical security process model.

ii) Output

What does specify the degree of implementation of the security controls? The survey addresses two aspects: the protection of critical business information and the ability to continue operations in the case of a disaster. Let us take question 30 and 38a to ask about the degree of implementation of security controls. Question 30 is: “In your opinion, how would you rate your organization's level of protection of its critical business information?”, and question 38a reads as follows: “How would you rate the ability of your organization to continue business operations in the event of a malicious attack or disaster?”.

The next output factor is about the number of security breaches and the ability to detect them. Question 32a asks: “How would you rate the ability of your organization to determine whether its information systems were under attack?”. Thus we can qualify the uncertainty of detecting a security event. The answers to question 35a yield facts about the actual security incidents: “To the best of your knowledge, has your organization experienced unexpected or unscheduled outage of a critical business system for more than two hours in the past twelve months?”.

The business strategy alignment is quantified by the answer to question number nine: “How well is your organization's information security spending aligned with its business objectives?”.

To complete the security process description we need data on how frequently security reports are sent to the higher management. Therefore we ask question number 13: “How often does your organization provide its board of directors or equivalent with a report about the organization's information security status or security incidents?”

3.2.1.3 CATEGORIZATION OF THE ANSWERS

Finally the answers must be quantified. It is very important to accurately categorize and value the answers. To avoid zero values, every scale begins with one. Every answer gets a value as it is shown in the following table. We just write down the beginning and the end of each scale.

Question	***Answer***	***Value***	***. . .***	***Answer***	***Value***
Question number 3: "How many employees are in your entire organization?"	few employees	1	. . .	Many employees	7
Question number 30: "In your opinion, how would you rate your organization's level of protection of its critical business information?"	not adequate at all	1	. . .	World class	5
Question number 38a: "How would you rate the ability of your organization to continue business operations in the event of a malicious attack or disaster?"	not adequate at all	1	. . .	World class	5
Question number 32a: "How would you rate the ability of your organization to determine whether your information systems were under attack?"	world class	1	. . .	Not adequate at all	5
Question number 35a: "To the best of your knowledge, has your organization experienced unexpected or unscheduled outage of a critical business system for more than two hours in the past twelve months?"	no	1	. . .	Yes	2
Question number 09: "How well is your organization's information security spending aligned with its business objectives?	no alignment	1	. . .	completely aligned	5

Question number 13: "How often does your organization provide its board of directors or equivalent with a report about the organization's information security status or security incidents?"	never	1	. . .	Monthly or more often	6

Table 3: The questions and the quantification of their answers

For some question there is the additional answer "not applicable". Fortunately no company makes use of this possibility and therefore we can use the information as it is, without further investigation and filtering.

3.2.2 THE EMPIRICAL MODEL

3.2.2.1 ASSUMPTIONS

The reality imposes some restrictions, e.g. data does not exist or the information available describes a factor slightly different than the original factor specification requires. So we are going to transform such facts into additional assumptions to get the basic model adapted to the real world situation.

i) Factors of Production

Unfortunately there is no information about the monetary expenditures and the manpower used to secure an ITIM. Thus we state that the sum of the IT security budget and the manpower used to secure an ITIM positively correlates with the system size.

ii) Incident Characteristics

Earlier we stated that for the protection analysis we are only interested in incidents that could have been avoidable. This means we just want to measure the negative security events that should have been preventable.

Now, for our analysis, we define that the answer to question number 35a is only about negative security events that should have been avoidable according to the security policy.

iii) System Size

Because the system size and the number of personal computers are not explicitly mentioned we declare that every worker has its own personal computer and the number of employees is equivalent to the number of personal computers.

3.2.2.2 REVISED INPUTS AND OUTPUTS

We rewrite the inputs and outputs according to the information we have gathered.

i) System – Input

The system size is the value of the answer to question number three:

SYS(X) = (value of answer to Q03, X asked), resp. SYS(X) $\in$ {1, 2, 3, 4, 5, 6, 7}; that means that the system size of company X is either 1, 2, 3, 4, 5, 6, or 7.

Using DEA we write:

$SYS_{DEAuc}(X) = 1/SYS(X)$, resp. $SYS_{DEAuc}(X) \in \{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \frac{1}{7}\}$. The appendix "$_{uc}$" tells us that SYS_{DEA} is an uncontrollable input.

ii) Factors of Production – Input

The answer of question number three is also used to describe the sum of the factors of production used:

FPROD(X) = RPROD(X) + STAFF(X) = (value of answer to Q03, X asked),

resp. FPROD(X) $\in$ {1, 2, 3, 4, 5, 6, 7}.

Please note that although FPROD(X) is proportional to SYS(X), FPROD(X) is not proportional to $SYS_{DEAuc}(X)$. Thus we cannot eliminate FPROD(X) and in DEA we write:

$FPROD_{DEA}(X)$ = FPROD(X), thus $FPROD_{DEA}(X) \in$ {1, 2, 3, 4, 5, 6, 7}

iii) Implementation – Output

Two pieces of information indicate the installed security controls and the degree of control implementation. These are the answers to question 30 and 38a and we take the mean of these two responses to describe the operating security controls of company X:

SECON(X) = ((value of answer to Q30, X asked) + (value of answer to Q38a, X asked)) / 2,

whereas (value of answer to Q30, X asked) $\in$ {1, 2, 3, 4, 5} and

(value of answer to Q38a, X asked) $\in$ {1, 2, 3, 4, 5}. So we get SECON(X) $\in$ [1, 5]

In DEA, the implementation output is set to:

$SECON_{DEA}(X)$ = SECON(X), and thus $SECON_{DEA}(X) \in$ [1, 5].

iv) Incidents – Output

Using the answer to question 32a we know how well a company detects a security event. The better the firm notices an incident the more sure we can be that the amount of incidents provided is accurate. Therefore we do rate the answer to question number 35a by the uncertainty supplied by the answer to question 32a:

RAIN(X) = (value of answer to Q32a, X asked) × (value of answer to Q35a, X asked), wheras X is the company under observation, (value of answer to Q32a, X asked) ∈ {1, 2, 3, 4, 5} and (value of answer to Q35a, X asked) ∈ {1, 2}. We work out that RAIN(X) ∈ [1, 10].
This factor as DEA output reads as follows:
$RAIN_{DEA}(X) = 1/RAIN(X)$, hence $RAIN_{DEA}(X) \in [1/10, 1]$.

v) Business Strategy Alignment – Ouput

Question nine seeks the business strategy alignment of organization X:
BSTRATSUPP(X) = (value of answer to Q09, X asked),
and BSTRATSUPP(X) ∈ {1, 2, 3, 4, 5}.
Because we can set $BSTRATSUPP_{DEA}(X) = BSTRATSUPP(X)$, we know that
$BSTRATSUPP_{DEA}(X)$ ∈ {1, 2, 3, 4, 5}.

vi) Reporting – Output

The 2003 IT security survey investigates the communication of the system protection status and security incidents to the strategic management:
REP(X) = (value of answer to Q13, X asked) and REP(X) ∈ {1, 2, 3, 4, 5, 6}.
Since $REP_{DEA}(X) = REP(X)$ we note that $REP_{DEA}(X)$ ∈ {1, 2, 3, 4, 5, 6} too.

3.2.2.3 THE EMPIRICAL SECURITY PROCESS MODEL

In accordance with the assumptions the reality enforces we define the so called empirical security process model.

$$\begin{pmatrix} SECON(X) \\ RAIN(X) \\ BSTRATSUPP(X) \\ REP(X) \end{pmatrix} = SecurityProcess \begin{pmatrix} SYS(X) \\ FRPOD(X) \end{pmatrix}$$

or

$$\begin{pmatrix} SECON_{DEA}(X) \\ RAIN_{DEA}(X) \\ BSTRATSUPP_{DEA}(X) \\ REP_{DEA}(X) \end{pmatrix} = SecurityProcess_{DEA} \begin{pmatrix} SYS_{DEAuc}(X) \\ FRPOD_{DEA}(X) \end{pmatrix}$$

Formula 8: Formal description of the empirical security process model

3.2.2.4 CONCLUSIONS

As we have seen, some information describing some factors have been found, some other data does more or less adequately characterize certain inputs and outputs, and specific facts do still lack. It is always a difficult task to extract information out of data that has been gathered with

different intentions in mind. For future analysis it would be beneficial to incorporate the security process point of view from the beginning. Nevertheless most of the information needed could be educed in some way from the IT security survey. Using some assumptions on the actual information provided we could adapt the basic security process model to the given data. The result of this is the empirical security process model.

3.3 THE IMPLEMENTATION: MAPPING DATA TO THE EMPIRICAL MODEL

We know now how and where to get the real world information that describes the input and output factors. Locating the facts needed has been the issue of the creation phase of the empirical process model. Now we are going to have a very close look at the true data. Sometimes the data itself can show signs of limitations, be it the quality or the availability.

3.3.1 ADJUSTMENTS

It could happen that some questions are not answered or that the interviewed assesses the asked subject as not applicable. In such cases we would annul the data of the corresponding organization. Fortunately the particular data given doesn't exhibit such problems. Each company has responded to the necessary questions that describe the inputs and outputs.
Calculating the data, one of the difficulties we could encounter are round-off errors. These problems may occur if the data isn't of similar magnitude across and within data sets[7]. These scaling issues don't affect us because our data is of similar size already.

3.3.2 CUSTOMIZATIONS

Looking at the data sets we find that we are talking about twelve interviewed organizations. That is a small amount in respect to the many input and output factors we have. To get enough discrimination in efficient and non-efficient units we should reduce the number of factors. Luckily we can decrease the amount of output factors without principally modifying the empirical security process model. We can combine the two aspects of protection, namely the implementation degree of the security controls and the avoidable negative security-related incidents. Preventable breakthroughs reflect a grievance of the installed security controls. These negative events indicate a substantial defect of the actual security control installation. We can say that having security troubles the defense of the security controls is decreased and the overall protection is lessened. We now introduce a new variable, call it protection (PROT) and calculate it as follows: PROT = SECON × (1/RAIN). Basically the protection is a positive output and it is indicated by the degree of the implementation of the security controls. The better the implementation is the more defense we have and the more protected we are. But

actual negativ security-related incidents lessen the protection. Thus by introducing the multiplier „1/RAIN“ we reduce the protection the more incidents we have. Because PROT is a positiv output the DEA version is $PROT_{DEA}$ = PROT. Referring to the basic security process model where SECON(*X*) ∈ [1, 5] and RAIN(X) ∈ [1, 10], we deduce that $PROT_{DEA}(X) \in [1/10, 5]$ for every organization X.

The next big issue is the strong relationship of the factors of production and the system size. This correlation will cause less diversity in the results. Having so few data sets we loose the expressiveness. To be able to do any DEA analysis we have to proceed without the factors of production. Thus we actually modify the empirical security process. We do alter the primal security process model. Cutting off FPROD(*X*) we get the new model and we do now only look at the output considering systems of different sizes.

3.3.3 THE DEA IMPLEMENTATION OF THE CUSTOMIZED EMPIRICAL SECURITY PROCESS MODEL

Now we have everything together to specify the DEA implementation of the customized empirical security process model. Due to the lacking availability of data the new model does only adress the output, cutting off the factors of production. In addition we eliminate the two outputs, the degree of implementation of the security controls and the number of avoidable incidents, and integrate the new protection variable. Now we set up the model taking the real world situation into account.

$$\begin{bmatrix} PROT_{DEA}(X) \\ BSTRATSUPP_{DEA}(X) \\ REP_{DEA}(X) \end{bmatrix} = SecurityProcess_{DEA} \begin{bmatrix} SYS_{DEAuc}(X) \end{bmatrix}$$

Formula 9: Formal description of the DEA implementation of the customized empirical security process model

Please note that previously we classified $SYS_{DEA}(X)$ as an uncontrollable input: $SYS_{DEAuc}(X)$.

3.3.4 THE IMPLEMENTATION - A SPREADSHEET

After intensive studies we are now able to realize the performance analysis. We have elaborated a modified and customized model of the security process that we can implement. So we know how to compute this construct. A spreadsheet containing the data is the base for the mathematical computation and the data evaluation.

4 APPLICATION PROCESS

4.1 SOFTWARE

There are many DEA software tools available. Some application software implement a lot of DEA models, some others compute just the basic ones such as the CCR and the BCC model. Other programs are written for developers and mathematicians. For this study it has come to the decision that a friendly user interface is of value allowing to concentrate on the problem itself rather than on the handling of the software. Frontier Analyst® from Banxia Software Ltd., United Kingdom, is a very easy to use professional DEA software tool providing all the functionality required and much more. Its analysis section is extensive and presents the results in a manner that is beneficial to the management.

4.2 COMPUTING

What are we going to compute? We want to know the efficiency of each organization in respect to the input and output factors defined; the inputs must be configured as controllable or non-controllable.

We have two models that we whish to address. For one thing there is the CCR model stating a constant return to scale relationship between the organizations. This means it is assumed that there is no scale effect active. For another thing we want to compare each organization to companies of similar scale size. For that purpose we use the BCC model that assumes a variable return to scale relationship between the different companies under observation.

There are two ways to identify the potential improvements and the efficiencies respectively: either by minimizing the input or by maximizing the output. At first we are interested in raising the output, especially the protection of the ITIM, without necessarily reducing the resources used. The input minimization is of secondary concern and could be discussed at a later date. Thus our goal is to maximize the output while fixing the input.

For now we take the spreadsheet containing the data and we compute both DEA models, the CCR and the BCC, maximizing the output. By the way we don't make use of the weighting functionality offered by the Frontier Analyst® software.

We do now the DEA analysis. There are twelve data sets; each containing four factors. In this case the computing time is about a second. We will discuss the resulting efficiency scores shortly.

5 DISCUSSION

5.1 MAIN ISSUES

Initially the idea was to look at the security process of IT based information systems by means of DEA and to find out if this analysis tool could help to understand and measure the security process. Unfortunately there was hardly anything that explicitly described the security process in a structured manner. Thus we first have had the additional task to create a security process model. Then we have developed an empirical model of the security process. The lack of data has caused the creation of a modified and customized security process model.
Now we are going to analyze the results. This output focused customized security model will be used to study aspects of the security process. We are not only trying to extract potential best practices; additionally we are looking for signs and hints that could asses the designed security process model as valid and the use of DEA as appropriate.

5.2 ASPECTS OF DEA

5.2.1 CONCEPTUAL APPLICABILITY OF DEA

While developing the basic security process model we stated that the DEA concepts were applicable to the security process designed. Furthermore we were able to adapt the basic security process model to the given data and thus to establish the empirical security process model. At the end we could have got a plausible DEA implementation of the security process model. Unfortunately the lack of data forced us to modify the primal security process model and to shift the view to the output. But overall DEA is conceptually applicable to the security process.

5.2.2 ADVANTAGES IN PRACTICE

One huge advantage of the DEA methodology is that it forces model builders to explicitly state the objectives of the processes and the assumptions made. For instance we have to describe the inputs and outputs in a structured manner and to define the modes of actions
Another plus are the peer based improvement targets. The potential improvements are based on the comparison to other organizations. Thus, taking the best producer as a standard, the targets aren't virtual at all and the potential improvements are realistic.

5.3 THE SURVEY – DATA DISCUSSION

5.3.1 THE SURVEY

5.3.1.1 THE SURVEY PROGRAM

The content of the surveys checked differs from year to year. The rate of change is about 60 percent. That means that a little bit more than half of the questions remain similar. Some issues were cut off and some other questions were introduced to explore new aspects of IT security. The questions of the aspects we are interested in are subject to the same rate of change. So it is a challenging task to establish a long-running analysis of our security process.

5.3.1.2 COVERAGE

About 17 percent of the questions of the survey in use provide answers to describe the security process. Some additional facts will be used to try to explain some security process characteristics. Altogether we use about a quarter of the questions interviewed and the responses given respectively.

5.3.2 QUESTIONNAIRE ISSUES

5.3.2.1 SUGGESTIVE ANSWERS

In the majority of cases we come across multiple-choice questions. Sometimes the possible answers given do have a valuation inherent. These answers are categorized by adjectives. If there is e.g. the choice between not adequate at all, inadequate, marginal, adequate and world class, most of the interviewers would reply adequate. Nobody wants to state e.g. to have a marginal accounting as well as hardly anybody will tell that the accounting is world class. Thus the persons asked often choose the same answer. This could diminish the prospect to classify the organizations in respect to that specific property.

5.3.3 THE DATA QUANTITY

Organizations manage their business in a multifaceted manner. The kind of operating and securing the information system infrastructure vary between different companies. Having only data of twelve companies makes it difficult to explore the different behaviors and to analyze the security process.

5.3.4 SUGGESTIONS

The analysis of the security process demands some specific information. Measurements gathered must be useful for describing the inputs and outputs. Thus the examination of the security process has its own demands.

It would be beneficial to get the specific questions into every questionnaire. So it would become possible to do a long-running study of the security process. Additionally questions that are more accurately in respect to the model could deliver a better description of the important factors.

5.4 THE ANALYSIS

It is of importance to have a good understanding of the security process and its model, especially the inputs and outputs, before interpreting any results. In particular we have even altered the security process model and have only one input factor, that is to say the size of the system. In addition it is essential to keep in mind that we have very few data sets. Finally let us consider that the quality of the responses depends on the maturity of an organization's security and controlling processes.

5.4.1 DATA REFERENCE

The data the results are based on was made available by Ernst & Young. Due to privacy considerations it is not possible to explicitly show the primary data as well as all the results. Details of this part of the analysis are just known to the author and Ernst & Young. The author asks you for your understanding.

5.4.2 PRELIMINARY STUDIES

5.4.2.1 POTENTIAL EXPLANATORY FACTORS

We are on the lookout for facts that could explain characteristics of the security process. The following information may be useful.

The compliance to laws plays a major role in the field of information security. Does compliance effectively support the security process or does it prevent us from implementing security efficiently? The Question number 18 addresses this issue: "Is your organization compliant with applicable security-driven regulations? (e.g., European Union's Data Protection Directive, the United Kingdom's Data Protection Act, and the HIPPA)".

Business is about communication. We talk to customers, exchange a few words there and have some discussions here. How well is the communication between the different business

units, especially between the IT unit and the business units? Does it have an influence on security? Therefore we ask question number 15: “In your organization, how often do the individuals responsible for information security meet with business unit leaders to understand their business objectives or information security needs?”.

A third important topic is the structured preparation of security actions. Do we have predefined rules to install security controls? Is there a plan about, a so called security policy? Does a good security policy promote system protection? Question number five reads as follows: “If you characterized your organization as either a ‘regional’ or ‘global’ entity in question 4, which statement best describes your information security policy structure? i) No formal global information security policies; individual or geographical or subordinate entities are free to develop own information security policies, ii) Global information security policies define the minimum set of rules needed to bind the organization together, iii) Global information security policies apply to the entire organization with additional policies applying to individual, geographical, or subordinate entities that are more restrictive, and iv) Others”.

Finally we want to find out how the companies see themselves. What kind of problems do they notice? Question 21, “In your opinion, what are some of the most significant obstacles to effective information security within your organization?”, asks about some awareness issues. From the many answers we focus on three items: i) Lack of formal information security management process or written policy, ii) Management commitment, and iii) Lack of ownership.

5.4.2.2 SENSITIVITY ANALYSIS

What have we done until now? We took the spreadsheet containing the data and we have computed both DEA models, the CCR and the BCC, maximizing the output using the customized empirical security model. To determine the stability of our customized security process model we have perturbed the data. First we have introduced a noise of 10 percent of the original data. Then we’ve disarranged the original data by 20 percent, and third we’ve messed it up with 30 percent perturbation.

We check the stability in respect to the efficiency. Is the change in the efficiency scores significant? Does data perturbation alter the order in respect to the efficiency? It follows that a variation of 10 percent of the original data doesn’t significantly change the results. More than 10 percent perturbation can cause alterations and a 30 percent deviation from the primary data doesn’t reflect the initial situation anymore.

5.4.3 RESULT EXAMINATION

5.4.3.1 GENERAL INSIGHTS

First we don't use any DEA results. Let us just look at the primary data of all companies. We see that compliance correlates with the effectiveness of protection (PROT): the more compliant a company is the more protection it actually has. Thus compliance could have an influence on the effectiveness of protection; the correlation is about 65 percent. Then we turn us to the reporting output (REP). We find that it is coupled with the intensity the IT unit communicates with the business leaders. The correlation of this communication frequency and the reporting output is about 80 percent, saying that the effectiveness of the reporting is positively affected by this intra-firm communication.

Now we glance at the group of organizations with good protection. Interestingly no organization has at least half of the protection possible. Again we see the above mentioned effects of the compliance and the unit leaders' communication. Unfortunately we cannot extract any further information about a potential good output combination; it seems that there are no specific rules or that the principles keep hidden.

5.4.3.2 SCALE EFFECTS

Now let us turn to the efficiency scores. Two models have been calculated: the CCR and the BCC model. The former model assumes that no scale effects are present, whereas the latter one compares the organizations to firms of similar scale sizes and hence addressing scale effects.

The customized empirical security process only shows the output in respect to the system size. Thus it would be unfair to compare organizations with other companies that operate on different scale size. Hence we are going to use the BCC model and thus we will only compare firms of similar scale size.

Using our customized security process model we can expect that larger companies will be more scale efficient than smaller ones. It would be interesting to learn more about. So we take the only input we have and analyze its interrelation with the scale efficiency. The expected strong correlation is about 90 percent: the smaller the company is the more scale inefficient it is. We even try to group the firms according to their system size and their scale efficiency respectively. We get four groups: the first group ranges from one to a thousand personal computers and their members are very scale inefficient, the second group goes from 1000 to 2500 pc's, the third from 2500 to 10000 pc's, and the fourth group consists of companies controlling more than 10000 pc's and being scale efficient.

It is important to note that scale inefficient does not mean inefficient at all. Although a company is scale inefficient, it can be efficient compared to other companies of similar scale size. The actual results show that every group has its efficient peer organizations. These organizations do run efficient within their sphere, even though they don't operate at the optimal scale size.

5.4.3.3 CLUSTERING

A company's transformation of inputs to outputs is compared to the transformation process of other companies. At the end of the DEA calculation there are one or more efficient companies that are standards for all other organizations. Every efficient organization has its followers and in turn every inefficient organization has its peer or its peer group. So we can build clusters consisting of an efficient organization as the center and the followers to this efficient organization. In our case using the BCC model a cluster contains organizations of similar scale size. Using the results we get six such clusters. Five clusters have about two to five members and one cluster consists of only its center.

5.4.3.4 CLUSTER SPECIFIC EXPLORATION

Now we take the efficient company with the largest protection and explore its cluster and thus its followers of similar scale size. Suddenly a lot of patterns do appear.

Foremost we recognize that the combination of the output factors isn't as arbitrary as first thought. The protection (PROT) is strongly related to the business strategy support (BSTRATSUPP). The correlation is about 80 percent telling us that better protection goes along with better business strategy support and vice versa. Even the reporting (REP) is slightly positive linked to the protection (about 30 percent) and to the business strategy support (about 15 percent). However the outcome tells us that protection and business strategy support are certainly no contradictory goals but complementary objectives.

In addition the results confirm the above mentioned positive relationship of compliance and protection as well as the positive interdependency of reporting and the intra-firm communication.

Turning to the efficiency scores we see an interesting pattern. The efficiency is strongly related to the protection (about 80 percent) as well as to the business strategy support (about 90 percent). Also good reporting output correlates with better efficiency. It seems that efficiency and good protection are complementary goals.

Now let us have look at the explanatory factors. The compliance and the intra-firm communication do not only have a positive correlation with the effectiveness of some output

factors, they even have constructive interrelations with the efficiency. The positive correlation between compliance and the efficiency is about 45 percent, and between the intra-firm communication and the efficiency about 70 percent.
It is interesting to see that in this specific cluster the efficiency is associated with the system size. The efficient organization, that is the center of the cluster, has a very small system. The bigger the system gets the less efficient the companies are. That could indicate that the bigger companies use tools and procedures that are not appropriate to their firm size.

5.4.3.5 SECURITY POLICY INFLUENCE

An exciting hypothesis is about the role of the security policy. It is said that a good security policy leads to good protection. Unfortunately most of the data sets don't contain an answer to the question addressing the security policy. So we just take the organizations that have an answer to the security policy question. In addition we only consider clusters with more than one member because we want to have organizations with a non-exotic output factor combination. Proceeding with the remaining units we see that the extent of the security policy is strongly related to the effectiveness of protection and that the security policy supports an efficient security process.

5.4.3.6 IMPROVEMENTS

The software tells us that the most improvement can be realized by augmenting the protection. We have already got a similar insight as we screened the protection of the companies: no firm reaches half the protection possible.

5.5 CONCLUSION

DEA is also applicable in practice. The method gives us very interesting insights into the security process. The DEA implementation of the customized security process is quite robust.
Once more it has to be reminded that we are talking about very few data sets and a modified and customized empirical security process. Hence we must look at the results very carefully.
It seems that some companies do not use the right tools regarding their size. Nonetheless the most improvement that is needed in order to become efficient is the increase of protection. Additionally it seems that protection and the business strategy support are complementary goals. The best practices to raise the effectiveness of protection and to improve the efficiency of the security process are the use of security policies and the aim to get compliant. Unfortunately the data tells us that most firms have a different awareness. They don't see the lack of a formal information security management as an obstacle; at least they don't prioritize

a formal information security management process, a written policy or management commitment.

Above all it is worthwhile to further track the security process idea and moreover to further analyze the application of DEA to the security of IT based information systems.

5.6 OUTLOOK

The models developed are a good starting point for further research in the field of the security of IT based information systems. There is a lot of interesting work to do. First this analysis should be repeated with more data. In addition different models of the security process could be developed and compared. How does the security process evolve over time? Windows analysis could also help to understand the security process. And why don't create an application to automatically identify potential improvements and then to provide companies with individual best practices?

Thank you for reading; I hope it was informative and enjoyable.

6 APPENDIX A – ACRONYMS

COMMON ABBREVIATIONS

ASSET Automated Security Self-Evaluation Tool[44]

The purpose of ASSET is to automate the completion of the questionnaire contained in NIST Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems."

BCC The BCC (ratio) model is the DEA model when a variable returns to scale relationship is assumed between inputs and outputs. It is named BCC after Banker, Charnes and Cooper. The BCC model measures technical efficiency. The convexity constraint in the model formulation ensures that the composite unit is of similar scale size as the unit being measured. The efficiency score obtained from this model gives a score which is at least equal to the score obtained using the CCR model[9].

CCR The CCR (ratio) model is probably the most widely used and best known DEA model. It is the DEA model used in Frontier Analyst when a constant return to scale relationship is assumed between inputs and outputs. It was the first DEA model to be developed, named CCR after Charnes, Cooper and Rhodes. This model calculates the overall efficiency for each unit, where both pure technical efficiency and scale efficiency are aggregated into one value[21].

CSD Computer Security Division, one of eight divisions within NIST's Information Technology Laboratory.

CSRC Computer Security Resource Center

This is the website of the Computer Security Division (CSD). The homepage can be found at http://csrc.nist.gov (reference date 04/10/2005)

FISMA Federal Information Security Management Act (FISMA) of 2002, United States of America

INFOSEC National Information Systems Security

ISO International Organization for Standardization (ISO)

ISO is a network of the national standards institutes of 156 countries, on the basis of one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system.

http://www.iso.org (reference date 05/10/2005)

IT Information Technology

ITIM	An information systems that is based on information technology (IT based information system), plural: ITIMs An ITIM is a sub system of the general class of information systems.
NIST	National Institute of Standards and Technology, United States of America The homepage is http://www.nist.gov (reference date 04/10/2005)
NSTISSC	National Security Telecommunications and Information Systems Security Committee, United States of America
SP-X	NIST Special Publications, provided by the CSRC http://csrc.nist.gov/publications/nistpubs/index.html (reference date 04/10/2005)

7 APPENDIX B – GLOSSARY

Accepted risk	The accepted risk is the potential loss an organization is willing to live with.
Aggregate efficiency	A term used to describe the measure of efficiency from the CCR model. Dividing the aggregate efficiency (from the CCR model) by technical efficiency (from the BCC model) results in the scale efficiency. A unit is "scale efficient" when its size of operation is optimal. If its size of operation is either reduced or increased its efficiency will drop. A scale efficient unit is operating at optimal returns to scale[10].
Availability	Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]
Business criticality	This is the relevance of the confidentiality, integrity and availability of an ITIM to the business. And it is incorporated into the risk calculation.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]
Critical success factors	These are the key areas where the organization must perform well to achieve the mission[20].
Defense planning	Planning risk mitigation actions
Information systems security (INFOSEC)	Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]

Risk	A measure indicating the endangerment of a system or asset conditioned by certain threat or threats respecting the environmental situation. It is calculated as the business criticality of the system/asset multiplied the probability the threat event occurs multiplied the impact the threat event can cause.
Security policy	The security policy is a list of the security controls that have to be installed to adequately protect the ITIM (or ITIMs), consistent with the business strategy and the accepted risk. The security policy is the plan saying how to reduce risk to an acceptable level and maintain that level of risk. The security policy is the result of the strategic processes and the base for the implementation of the safeguards.
Security process	The security process is the process that transforms an ITIM into a risk adequate secured ITIM that is consistent with the defined business strategy and within accepted risks.
Technical efficiency	A unit is said to be technically efficient if it maximizes output per unit of input used. Technical efficiency is the efficiency of the production or conversion process. Technical efficiency is calculated using the BCC model (a kind of DEA models). The impact of scale size is ignored as "decision making units" (DMU's) are compared only with units of similar scale sizes[10].
Threat	A possible event or occurrence, emerging at a certain probability that has the potential to compromise the security of a system or asset[26].

8 APPENDIX C – REFERENCES

[1] **Accenture**, How the Right IT Metrics Can Contribute to High Performance, http://www.bettermanagement.com/library/library.aspx?libraryid=12425&pagenumber=1 (reference date 03/10/2005)

[2] **Andrew Briney**, CISSP, What is enough security?, 06.10.2004, http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci969709,00.html (reference date 19/10/2005)

[3] **Asia Hussain and Jennifer R. Brightman**, Frontier Analyst – White Paper: Frontier Analyst in depth, Banxia Software Ltd., UK http://www.banxia.com (reference date 03/10/2005)

[4] **Asia Hussain**, Matthew Jones, Frontier Analyst – An Introduction to the Frontier Analyst, Frontier Analyst Workbook 1, Version 1.1, April 2001, Banxia Software Ltd, Kendal, Cumbria, UK

[5] **Avkiran Necmi K.**, An application reference for data envelopment analysis in branch banking: helping the novice researcher, International Journal of Bank Marketing, 1999, Vol. 17 Issue 4/5, 206-220

[6] **Avkiran Necmi K.**, Productivity Analysis in the Service Sector – with Data Envelopment Analysis, Second Edition, 2002, The University of Queensland, ISBN 0-9580550-0-9, p. 175

[7] **Avkiran Necmi K.**, Productivity Analysis in the Service Sector – with Data Envelopment Analysis, Second Edition, 2002, The University of Queensland, ISBN 0-9580550-0-9, p. 198

[8] **Bank for International Settlements**, The Application of Basel II to Trading Activities and the Treatment of Double Default Effects, April 2005, http://www.bis.org/publ/bcbs111.htm (reference date 03/10/2005), Basel Committee on Banking Supervision

[9] **Banker, Charnes and Cooper**, Management Science, 1984, Vol. 30/9, pp. 1078-1092

[10] **Banxia Software Ltd**, DEA Glossary, Frontier Analyst, Kendal, Cumbria, UK, http://www.banxia.com/frontier/glossary.html (reference date 13/10/2005

[11] **Banxia Software Ltd., UK**, Frontier Analyst – Help File

[12] **Berinato Scott**, Global Security Survey ´04, September 15, 2004, CIO Magazin, PriceWaterhouseCoopers

[13] **Blumenberg Stefan**, Dipl.-Kfm., Benchmarking Financial Processes with Data Envelopment Analysis, Institute for Information Systems at Frankfurt University

[14] **Brightman Jennifer R.**, Banxia Software Ltd., UK

[15] **Briney Andrew**, What is enough security?, CISSP, 06.10.2004, http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci969709,00.html (reference date 04/10/2005)

[16] **BSI**, Kurzinformationen zu aktuellen Themen der IT-Sicherheit, Bundesamt für Sicherheit in der Informationstechnik (Germany), http//www.bsi.de (reference date 03/10/2005)

[17] **Cabinet Office, UK**, Security - e-Government Strategy Framework Policy and Guidelines, Version 4.0, September 2002, Office of the e-Envoy

[18] **Carnegie Mellon University**, How Much Security Is Enough?, Governing for Enterprise Security, CERT Coordination Center, Software, Engineering Institute, Pittsburgh, PA http://www.cert.org/governance/adequate.html (reference date25/10/2005)

[19] **Carnegie Mellon University**, SQUARE Project: Cost/Benefit Analysis Framework for Information Security Improvement Projects in Small Companies, System Quality Requirements Engineering (SQUARE) Team, Technical Note CMU/SEI-2004-TN-045, November 2004, http://www.sei.cmu.edu/publications/index.html (reference date 02/11/2005)

[20] **Carnegie Mellon University**, The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Management, CMU/SEI-2004-TR-010, ESC-TR-2004-010, July 2004, Software Engineering Institute, Pittsburgh, PA

[21] **Charnes, A., W.W. Cooper and E. Rhodes**, Measuring the Efficiency of Decision Making Units, European Journal of Operational Research 2 (1978), 429-444.

[22] **Christopher Michael**, An Introduction to NIST's Security Framework, CSI 31st Annual Security Conference and Exhibition, November 9, 2004, Washington D.C., Computer Security Institute, http://www.gocsi.com (reference date 05/10/2005)

[23] **Common Criteria Portal**, Common Criteria: An Introduction, www.commoncriteriaportal.org (reference date 03/10/2005)

[24] **Emrouznejad, A.,** Data Envelopment Analysis Home Page, http://www.DEAzone.com (2003) (reference date 03/10/2005)

[25] **Ernst & Young**, Information Security Survey: Global Report, EYG No. FF0231

[26] **Government of Canada Publications**, ITSG-MG2, IT Security Guidance, Canada, http://www.cse-cst.gc.ca/en/publications/gov_pubs/itsg/itsg-e.html (reference date 18/10/2005)

[27] **Growth Management Strategies, LLC**, Business Strategy, Wayne, PA, http://www.ss-designs.com/gms/busstrat.htm (reference date 18/10/2005)

[28] **Horton Thomas**, Ph.D., Charles Le Grand , CIA, CISA, CDP, William Murray, Will Ozier, President, OPA Inc., Donn Parker, The Institute of Internal Auditors, Altamonte Springs, Florida, Managing Information Security Risks - Part 1, Risk Management, Vol. 3, August 15, 2000, http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=250 (reference date 30/10/2005)

[29] **Hussain Asia and Brightman Jennifer R.**, Frontier Analyst – White Paper, Banxia Software Ltd., UK
http://www.banxia.com (reference date 03/10/2005)

[30] **Information Security Decisions Conference**, October 19-21, 2005, NY City, Information Security Decisions, c/o TechTarget, Needham, MA,
http://infosecurityconference.techtarget.com/
(reference date 04/10/2005)

[31] **Information Security Forum (ISF)**, The ISF's Standard of Good Practice,
http://www.isfsecuritystandard.com (reference date 03/10/2005)

[32] **Information Systems Audit and Control Association (ISACA)**, A Framework for Information Security Governance – The Federal Perspective, A paper submitted to the San Francisco Chapter of the Information Systems Audit and Control Association (ISACA),
Mike Nelson, CISSP, CISM, MBA, President SecureNet Technologies, Inc.
http://www.securenet-technologies.com (reference date 05/10/2005)

[33] **International Organization for Standardization (ISO)**, Information Security,
http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html (reference date 19/10/2005)

[34] **International Organization for Standardization (ISO)**, ISO 17799, Information technology - Security techniques - Code of practice for information security management,
http://www.iso.org (reference date 05/10/2005)

[35] **International Organization for Standardization (ISO)**, ISO/IEC 17799,
http://www.iso.org (reference date 03/10/2005)

[36] **Lien Donald and Peng Yan**, Measuring the efficiency of search engines: an application of data envelopment analysis, Applied Economics, 1999, 31, 1581-1587

[37] **More Than Computers, Inc. (dba) Inacom Information Systems**, Madison, WI,
http://www.inacom.com (reference date 04/10/2005)

[38] **Parkin David and Hollingsworth Bruce**, Measuring production effciency of acute, hospitals in Scotland, 1991-94: validity issues in data envelopment analysis, Applied Economics, 1997, 29, 1425-1433

[39] **Security Matrix Inc.**, Orlando, FL, http://www.security-matrix.com (reference date 05/10/2005)

[40] **SOX-Online**, http://www.sox-online.com (reference date 03/10/2005)

[41] **Spitzner Lance**, Steering Committee Research Alliance, The Honeynet Project
http://project.honeynet.org/index.html (reference date 19/10/2005)

[42] **Stephen O'Grady**, SOA Meets Compliance: Compliance Oriented Architecture, RedMonk Study 12th August 2004, Denver, CO

[43] **U.S. Department of Commerce**, Annual Report 2003, Computer Security Division (CSD), National Institute of Standards and Technology, Technology Administration

[44] **U.S. Department of Commerce**, ASSET – Automated Security Self-Evaluation Tool, Computer Security Division, National Institute of Standards and Technology, Technology Administration, http://csrc.nist.gov/asset (reference date 16/11/2005)

[45] **U.S. Department of Commerce**, FIPS 199, February 2004, Federal Information Processing Standards Publications, National Institute of Standards and Technology, Technology Administration

[46] **U.S. Department of Commerce**, FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, July 2005, Federal Information Processing Standards Publications, National Institute of Standards and Technology, Technology Administration

[47] **U.S. Department of Commerce**, NIST SP 800-12, An Introduction to Computer Security: The NIST Handbook, National Institute of Standards and Technology, Technology Administration

[48] **U.S. Department of Commerce**, NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems, December 1998, National Institute of Standards and Technology, Technology Administration

[49] **U.S. Department of Commerce**, NIST SP 800-26, Security Self-Assessment Guide of Information Technology Systems, National Institute of Standards and Technology, Technology Administration

[50] **U.S. Department of Commerce**, NIST SP 800-27 Rev A, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A, June 2004, National Institute of Standards and Technology, Technology Administration

[51] **U.S. Department of Commerce**, NIST SP 800-30, Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, Technology Administration

[52] **U.S. Department of Commerce**, NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004, National Institute of Standards and Technology, Technology Administration

[53] **U.S. Department of Commerce**, NIST SP 800-53, Recommended Security Controls for Federal Information Systems, February 2005, National Institute of Standards and Technology, Technology Administration

[54] **U.S. Department of Commerce**, NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems, July 2005, National Institute of Standards and Technology, Technology Administration

[55] **U.S. Department of Commerce**, NIST SP 800-55, Security Metrics Guide for Information Technology Systems, National Institute of Standards and Technology, Technology Administration

[56] **U.S. Department of Commerce**, NIST SP 800-60, Version 2.0, Guide for Mapping Types of Information and Information Systems to Security Categories, National Institute of Standards and Technology, Technology Administration

[57] **U.S. Department of Commerce**, NIST SP 800-70, Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers, May 2005, National Institute of Standards and Technology, Technology Administration

[58] **U.S. National Instutiute of Standards and Technology**, NIST – Special Publications, Computer Security Ressource Center (CSRC), http://csrc.nist.gov (reference date 03/10/2005), Computer Security Division

[59] **U.S. National Instutiute of Standards and Technology**, NIST SP 800-53, Appendix G, February 2005

[60] **U.S. National Security Telecommunications and Information Systems Security Committee**, National Information Systems Security (INFOSEC) Glossary, NSTISSI No. 4009, September 2000

[61] **U.S. Public Law**, Federal Information Security Management Act of 2002, Title III of the U.S. E-Government Act, Public Law 107-347

[62] **U.S. Public Law**, Gramm-Leach-Bliley Act, U.S. Public Law 106-102, 15 U.S.C. § 6801, et seq.

[63] **U.S. Public Law**, Health Insurance Portability and Accountability Act of 1996, U.S. Public Law 104-191

[64] **U.S. Senate and House of Representatives**, Sarbanes-Oxley Act of 2002

[65] **United States Code**, [44 U.S.C., Sec.3542], Office of the Law Revision Counsel, United States of America, http://uscode.house.gov (reference date 05/10/2005)

[66] **Vitaliano Donald F.**, Assessing Public Library Efficiency Using Data Envelopment, Annals of Public and Cooperative Economics 69:1 1998 pp. 107-122

[67] **von Bergen S.**, Data Envelopment Analysis - Theoretische Grundlagen, Entwicklung einer Benutzeroberfläche in Delphi und Anwendung auf Spitaldaten, 2003, Institute for Operations Research, University of Zurich

[68] **Waters John K.**, Can the hackers be stopped?, http://www.adtmag.com/article.asp?id=6401 (reference date 19/10/2005)

[69] **Zhu Joe**, DEAFrontier - A "Data Envelopment Analysis Home Page", http://www.deafrontier.com (reference date 03/10/2005)

[70] **Zhu Joe**, Quantitative Models for Performance Evaluation and Benchmarking: Data Envelopment Analysis with Spreadsheets and DEA Excel Solver, Kluwer Academic Publishers, Second Printing 2004