Security Scandinavian Style

Interpreting the Practice of Managing Information Security in Organisations

Fredrik Björck

DSV Department of Computer and Systems Sciences

Stockholm University /
Royal Institute of Technology

Report series
No. 01-017
ISSN 1101-8526
ISRN SU-KTH/DSV/R--01/17--SE

Submitted to Stockholm University in partial fulfilment of the requirements for the degree of Licentiate of Philosophy

Security Scandinavian Style

Interpreting the Practice of Managing Information Security in Organisations

Fredrik Björck

Licentiate Thesis

2001

Stockholm University & Royal Institute of Technology

Publication Data:
Fredrik Björck
Security Scandinavian Style - Interpreting the Practice of
Managing Information Security in Organisations
Stockholm: Department of Computer and Systems Sciences
Stockholm University & Royal Institute of Technology
Report series No.01-017, ISRN SU-KTH/DSV/R--01/17--SE
ISSN 1101-8526

— In Memory of Professor Bengt G. Lundberg —

Abstract

This thesis presents the findings of an empirical study into the evaluation, formation and implementation of information security management systems aiming to protect organisational information assets. An action research oriented strategy and a research method informed mainly by grounded theory, are employed. The main elements of this thesis are 1) a blueprint process for information security management, 2) an information security evaluation method, 3) sucess factors for creating balanced information security management systems, and 4) a discussion on problems related to measuring the effects of information security education in an organisational context.

Acknowledgements

Louise Yngström, my advisor and mentor; for taking me on as a doctoral candidate, for introducing me to key information security players in Sweden, in Europe and on the international arena, for pressuring me with deadlines and at the same time giving me the freedom to grow.

Swedish Standards Institutes' information security management systems project, especially Jan-Olof Andersson (Sveriges Riksbank) and Inger Nordin (Validation AB); for giving us the opportunity to study the management of information security in the context of the ISO/IEC 17799 standard.

The Swedish Information Processing Society, especially Mats Lundquist (product manager for SBA); for excellent cooperation, and for making some of the ideas presented in this thesis available to practitioners through courses and software.

My colleagues and friends. My family.

Thank you.

CONTENTS

LIST OF FIGURES

1. INTRODUCTION

1.1 Background to the research

Too much business security will increase your costs and reduce your potential revenue streams substantially (*ceteris paribus*) and it can - in due course - put an end to your business. To "run the risk" is in fact at the heart of entrepreneurship; American economist Knight pointed out that "profit, earned by the entrepreneur who makes decisions in an uncertain environment, is the reward for bearing uninsurable risk" (Knight 1921). Conversely, insufficient security might leave your business open for fatal mistakes, espionage, sabotage and crime. The goal of security management in organisations should therefore be to identify and strive toward the optimal point between security and insecurity.

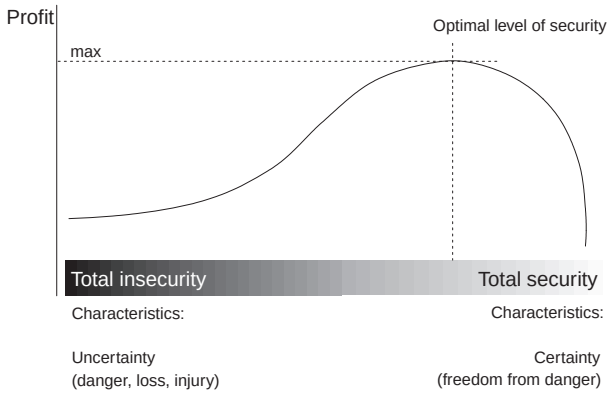


Fig. 1.1: *The optimum level of security – illustrating the balancing act of security management.*

The optimum level of security in an organisation (Fig. 1.1), from a strict financial perspective, will be found in the situation were the cost of *additional* security countermeasures *exactly equals* the *resulting* reduction in damages arising from security breaches (Marin 1992). This level of security means profit maximisation for the organisation. Too little security means that security breaches are reducing profits as a result of damages to assets, and too much security means that the costs of security countermeasures (including operational ineffectiveness and high-end security solutions) consume profits (Björck 1996). Hence, we should

not strive towards higher and higher security without thinking about the consequences. Moreover, security measures have other consequences than strictly monetary to be taken into account, *e.g.* social, legal and ethical. Opposing views from various groups of stakeholders to the organisation will also have to be recognized.

In practice, it is problematical to identify the security equilibrium depicted here. In many cases, the total cost of current security countermeasures and the damages arising from current security breaches, are not known. And, looking into the future, the potential costs-and-benefits of new countermeasures are even more challenging to estimate (Adams 1995). To further complicate things, this research is not on protecting organisational assets in general – it is about protecting *information assets*. It is difficult to assess the value of a given information asset, since it mainly depend on what it can be used for in the future (Falk and Olve 1996, Glazer 1993). Also, it is not always noticeable that an information asset has been subject to a security breach – if it *e.g.* has been changed by mistake or disclosed to an unauthorized party. As a result, it is problematic to devise economically optimised information security measures.

It is widely agreed that organisations in reality do not behave strictly according to a profit-maximising economic model (as that in Fig. 1.1). Instead, decisions and behaviour are characterised by, at best, bounded rationality and trying to satisfy objectives rather then reaching them (Simon 1947, Cyert and March 1963). Hence, it is important to keep in mind that the model used here is an *ideal model* from the point of view of the owners of the organisation, aiming to clarify the problems faced.

Despite the difficulties outlined above, organisations need to at least try to estimate; a) the current level of information security, b) the ideal level of information security, and c) how to get from *a* to *b*. Although this research will not conclusively *solve* any of these issues, it is concerned with all three.

Several recent studies demonstrate the need for organisations to systematically approach the protection of their information assets:

- Computer Economics estimates that for 2001 (as of the end of August) the economic impact of virus attacks around the world has hit $10.7 billion (Computer Economics 2001)
- 85% of the 528 U.S. organisations responding to the annual CSI/FBI survey detected computer security breaches within the last twelve months and 64% acknowledged financial losses due to those breaches (CSI 2001)
- 66% of the 273 European CIOs and business executives interviewed in the most recent Ernst & Young Information Security Survey cite information security or privacy concerns as a major inhibitor to greater use of e-commerce (Ernst & Young 2001)
- In Sweden, 84% of the respondents (*n=428*) to the most recent Information Security Survey had suffered economic losses due to breaches of information security, as compared to only 56% of the respondents (*n=541*) the year before (Björck 1997, 1998).

Adding to this the rapidly increasing dependence of information and IT systems, the need to manage information security is apparent.

1.2 Research questions

The research tackles certain aspects in connection with the following question:

> *What problems do organisations face, and what processes do they go through, as they are aiming to establish a balanced management system for information security?*

This question does not have *one* answer - it has *many*: Organizations have different goals, strategies, organisational cultures and -structures, consequently the ideal management system and the way to achieve it will differ between organizations (Mintzberg 1983). Acknowledging this - the need to cater for situational context - this thesis proposes a framework instead of a comprehensive information security management methodology. Organisations and researchers can use the framework to "plug-in" preferred approaches, fitting to the context of the problem at hand. Beyond the framework, the thesis deals with sub-problems within the broad research question. It also attempts to build a tentative "plug-in" methodology for a part of the framework.

In correspondence with the research question above, the framework for the thesis - presented in detail in chapter 3 - is a process view of the activities included when an organisation seeks to arrive at a balanced management system for information security. Henceforth, we shall refer to this as the information security management system (ISMS) process. A high level view is presented here to illuminate how the *specific research questions* contribute to the study at large (figure 1.2). Each of the revised and extended papers presented in the thesis'

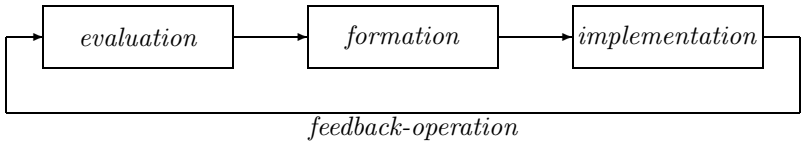


Fig. 1.2: *The Information Security Management Process (ISMS Process).*

main body is positioned within one of the three main stages of the ISMS process – *evaluation*, *formation*, and *implementation* (please refer to the next chapter for a detailed description of these).

The research question related to the *evaluation stage* of the ISMS process is:

> *1) How can an organization evaluate its current state of information security?*

This question is answered by offering a tentative evaluation methodology and an associated software tool. The Swedish Information Processing Society and leading information security experts in Sweden, in close cooperation with this research project, designed and built the software tool. The evaluation methodology was developed as a part of this study. This work is presented in chapter four.

The research question related to the *formation stage* of the ISMS process is:

> *2) What are the success factors to consider while creating a management system for information security?*

The answer to this question is sought using questionnaires to certification auditors and information security consultants all working in projects aiming to create management systems for information security corresponding to the ISO/IEC 17799 standard (ISO 2001). This work is presented in chapter five.

The research question related to the *implementation stage* of the ISMS process is:

> *3) What problems are related to measuring implementation effectiveness of information security education efforts?*

This question is mainly tackled analytically using simple ROI-models (return on investments) from financial economics to illustrate the problem of measuring implementation effectiveness with regards to the human side of the information security management system. This work, parts of which are co-authored with Yngström is presented in chapter six.

The ISMS process, as described here and in detail in the following chapter, illustrates a range of problems and promising solutions to many activities involved in evaluating, forming and implementing a management system for information security in an organisation. The intention is not to present it as the main *result* of this study. The framework should be viewed as an *ideal model* meaning that *it does not claim* that "this is the way all organisations do", or "this is the way all organisations have to do". Rather, it serves as a *framework* for the thesis pointing out critical problem areas that are investigated and indicating how these fit together. It is also important to note that this study does not solve all problems in the ISMS process – it merely confronts some of these.

1.3 Justification for the research

The current state of - and the ensuing need for - information security was demonstrated earlier (section 1.1) by referring to several recent studies. In addition, the development of information security management on the international and national (Sweden) arena further accentuates the need for this study:

ISO, International Organization for Standards, recently promoted the British standard on information security management (BSI 1995, 1999) to an international standard, ISO/IEC 17799 (ISO 2001). Many organisations are now

striving to meet the requirements of the standard. To do this, they will have to demonstrate that they have a management system for information security that is adequately protecting their information assets. The standard does not mention, however, *how* this can be attained. That is exactly the focus of this study. In Sweden; since the beginning of 1998, the Swedish Standards Institute (SIS) has worked to create and market a Swedish version of the cited British standard (BSI 1995, 1999). It succeeded in 1999, when Sweden as one of the first countries adopted it as Swedish Standard 62 77 99 (SIS 1999a, b). As a part of this undertaking, SIS formed a *pilot certification group*, later reformed into an *experience group* aiming to better understand and interpret the requirements of the standard and – especially - *how* to achieve them. We have been documenting the experiences in these groups as a part of this study.

On the academic level, the aim of this undertaking is to contribute to the body of knowledge regarding information security management in organisations. This contribution will mainly be in the form of helping increasing the understanding of problems associated with the ISMS process. In addition, it is hoped that this study can fill a gap by presenting the issues from a Scandinavian perspective. In our view, different nations seem to interpret information security management in different ways, often directly corresponding to the existing corporate culture and management style.

During the course of this study, results have continuously been fed back to information security management practitioners and scholars through different channels. The aim was to test the usefulness and relevance of the findings. The software tool presented in chapter four is now internationally available, through the Swedish Information Processing Society, to users - in both Swedish and English (SIPS 2001). As of September 2001 it has over 200 licensed users, mainly Swedish organisations. Over 100 information security managers and consultants have attended courses in using the evaluation methodology associated with the software tool (in the latest course, 100% of those attending rated the course contents as "good" or "very good" in a course quality survey). The success factors presented in the *formation* chapter (five) have been fed back to information security practitioners in Sweden at various industry conferences and as a publication from the Swedish Standards Institute (see Swedish reports enclosed in appendices). Major parts of this study have been accepted and presented at international academic conferences on information security in Sweden, Australia, China, and the USA. In summary, we feel that the partial results fed back so far have proved valuable to both academia and practice. Therefore, it is our anticipation and aspiration that this work - now presented in its entirety - will prove useful and relevant to these two audiences.

1.4 Summary of contributions

1.4.1 Contributions related to information security management in general

By modelling the ISMS process - with the stages *evaluation, formation,* and *implementation* - we have provided a blueprint process against which organisa-

tions attempting to attain a management system for information security can benchmark their current practices. The proposed ISMS process may also serve as a didactic instrument in education and training for explaining the interdependent activities involved in information security management. On a more general level, this study has showed that information security management is not only about technicalities and engineering, but also about the human side of enterprise – people. Hence, one contribution is that it has helped to shift the focus away from computer system security to information (systems) security.

1.4.2 Contributions related to the evaluation of information security and ISMSs in organisations

By offering a tentative evaluation methodology and associated software tool, we have already started to fill in the details of the ISMS process. By explicating the methodology and the ideas behind it, and by building in flexibility in the software tool, organisations that feel that the methodology does not suit their corporate culture or evaluation situation can adapt it to better suit their needs.

1.4.3 Contributions related to the formation (design, development) of information security management systems in organisations

This study has contributed through identifying a set of success factors associated with the formation of management systems for information security in organisations. Organisations facing this challenge will probably find this relevant and beneficial, since it enables them to avoid now recognized pitfalls and capitalize on known winning techniques. Moreover, the hunt for success factors showed that the core problems associated with creating an information security management system is akin to those problems confronted in any organisational change effort. This might be viewed as a contribution in itself, since it opens up a whole new avenue of theories, tools and methods for information security management.

1.4.4 Contributions related to the implementation of information security management systems in organisations

We contributed through identifying the problems associated with measuring effectiveness of education programmes as a part of the implementation of information security management programmes in organisations. Specifically, the main contribution of this part was to identify the need for measuring the effects of education and training in this context, and also pointing out some major obstacles *vis-à-vis* measuring. The papers also shows the consequences of many organisations' fixation to "monetarize" and compare their investments, including those into knowledge.

1.5 Quality and limitations of this work

Lincoln and Guba (1985) proposed four concepts that taken together may be used to demonstrate the soundness of a qualitative research approach – credibility, transferability, dependability, and confirmability:

1.5.1 Credibility aspects

> *Credibility - do the findings presented in this thesis accurately reflect the reality studied?*

Social reality is not a fixed reality that we can go out and study. On the contrary – it is a constantly moving target – and it is constantly being constructed. For that reason, there is no *one* reality, and therefore not only *one* truth about it that we can hope to find. Instead, there are multiple realities and multiple views. The question of credibility then is the question of if this study is "credible to the constructors of the original multiple realities" (Lincoln and Guba 1985:296). As will be demonstrated in the next chapter, results of this study have been fed back on a continuous basis to these "constructors" to ensure that what is written in this thesis gives a truthful account of the studied phenomena. However, we acknowledge that the background and pre-understanding on the part of the researcher does *influence* the findings, and especially how these are presented.

1.5.2 Transferability aspects

> *Transferability – are these findings useful for to others in similar situations?*

A qualitative research design, like this, makes it problematic to generalize findings back to a stated population. On the other hand, it gives a much richer and deeper understanding and description of the studied phenomena. It is important to point out that this study cannot, and should not, be taken as a description of how "it is" in *all* organisations – that was not the intention. On the ideographic – nomothetic dimension, this study does not search for general laws of information security management (nomothethic) – no, it looks to describe specific problems, processes, and events, so that we can better understand these (ideographic). Nevertheless, if this knowledge could not be of use for others, it would not be worth the effort. By stating the boundaries and contexts within which this study has been undertaken, the reader can judge weather this knowledge could be of any use in another situation. Given that this thesis is based on a Scandinavian perspective and organisational culture, it might prove more valuable to organisations with similar values and management styles.

1.5.3 Dependability aspects

> *Dependability – would the results be repeated if the study was replicated?*

Dependability is corresponding to what in natural sciences is called *replicability*, which is the extent to which an application of equivalent instruments to the same units yields similar results. Since qualitative studies by their nature cannot be replicated, because of changing realities, the attention is turned to the stability and consistency of the inquiry process. Dependability for this study can be determined by auditing provided descriptions on data collection and analysis, studying the data itself, and contrast this to the findings. So even though replicability seems impossible, there are still methods to judge the soundness of this study. Replicability is problematic in all studies, since everything in our world changes, and since it is difficult to ensure that the instruments (like a microscope) and processes used in the re-inquiry are sufficiently equivalent to those used in the original inquiry.

1.5.4 Confirmability aspects

Confirmability – do the data help confirm the findings?

As discussed above, objectivity on the part of the researcher seems problematic. Still, we need to be assured that the findings are not only the imagination of the researcher. Using a qualitative research design, we do not depend on the researcher's objectivity – instead we turn our attention to the data or empirical materials. Were possible, we have tried to include the data directly in the thesis, such as the numerous quotations in chapter 5. In other parts, data is available on request, such as in the case of chapter 7. There are parts, however, were it is difficult to provide data, since they build on an extensive period of participant observation. Although there are notes and documents from meetings, they do not give the full picture of the empirical materials gathered. In these cases, such as in chapter 4, it is still possible to confirm the soundness of the findings by going back and asking other persons that have been partaking in the same group or project. Even though we have done our outmost to ensure that everything written in this thesis is in line with the interpretations of the informants, it should be pointed out that the text in this thesis is also an interpretation - of that first interpretation.

1.6 Further work

Evaluation and refinement of SBA Check. As it stands, SBA Check and the evaluation approach presented in chapter 4 is not formally evaluated. The first step in this direction would be a survey to all licensed users of the software, focusing on the use of the tool, the perceived efficiency, the results, *etc.* A study like this, in cooperation with the Swedish Information Processing Society, is in its design phase right now. It will be carried out during 2002.

Interview with experts. Another idea that has grown stronger during this study is to interview acknowledged experts on the management of information security in organisations, and to analyse these interviews in line with the ideas of grounded theory to search for themes and patterns in their views on the issue at hand.

Case study in organisation. Most of the material presented in this thesis is *general* in the sense that it does not *directly* tackle the sometimes-chaotic reality in which organisations have to try to solve their information security problems (this study, as explained in section 2.2, has been on another level). In the practical situation, were abstract methods and loosely described security measures have to be interpreted and transformed into reality, other problems often emerge. Therefore, it would be very valuable to study various organisations in their efforts to manage information securely.

1.7 Outline of the thesis

The next chapter (2) outlines the research strategy and chapter 3 describes the framework used to unify the different parts of the thesis. These two chapters form the base of the thesis. Readers mainly interested in practical utilisation and application of the findings can pass over chapter 2 and go directly to chapter 3 where the information security management systems process model is described. Chapters 4, 5, and 6, each presents aspects of *evaluation*, *formation*, and *implementation* (respectively) – this is where the main studies of the thesis are presented. Chapter 7 through 10 entails various appendices.

2. RESEARCH STRATEGY AND RESEARCH METHODS

2.1 The choice of a research strategy

The management of information security in organizations has been fruitfully studied using a variety of research strategies, such as action research, case studies, and surveys[1]. The best possible research strategy to adopt is affected by number of factors, including; fundamental epistemological and ontological assumptions, the research context and the unit of analysis, and, logically, the research problem and –objective (figure 2.1).

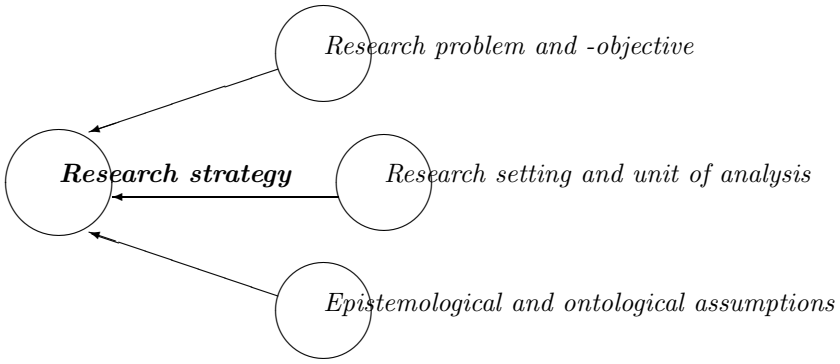


Fig. 2.1: *Factors affecting the choice of a research strategy*

Following is an explanation of how these factors have affected our choice to adopt an adapted version of *action research* as our basic strategy in this thesis.

Type of research problem and -objective. Barring for the chapter concerning the implementation stage, the different parts of this thesis describe research endeavours and results that are mainly of an *inductive* nature. The point of departure is the problems that organizations face, and the processes they go through, as they are aiming to establish a balanced information security management system. The approach is essentially *explorative* and *descriptive*, aiming to discern and understand these problems and processes.

[1] Refer to appendix A for a demonstration and discussion on different approaches and research foci in information security.

Research setting and unit of analysis. Empirical materials (data) are elicited from project groups formed with the purpose of discussing, understanding, and suggesting answers to these problems for practitioners. The findings presented in this thesis are based on our participation in these groups over the course of circa two years. The nature of our partaking, that is, to participate as researchers, was explicated and agreed upon at the outset. The participation has - with intent - been one of active involvement, not only as observers, but also as active group members.

Fundamental epistemological and ontological assumptions. This research is built on an underlying *interpretive epistemology*, in that we assume that the management of information security in organisations ideally should be explored from the frame of reference of those who are directly involved in these processes. Hence, this research could be classified within what Burell and Morgan (1979) would call the interpretive paradigm:

> The interpretive paradigm is informed by a concern to understand the world as it is, to understand the fundamental nature of the social world at the level of subjective experience. It seeks explanation within the realm of individual consciousness and subjectivity, within the frame of reference of the participant as opposed to the observer of action. (Burell and Morgan 1979: 28)

Our ontological stance is that the social world, which forms substantial parts of an organization, does *not* exist independently of the observer. Managing information security in organizations is mainly about trying to control certain aspects of the social world, through influencing human behaviour *a propos* information security. Likewise, a decision to change the security of a computer based information system has to be interpreted and carried out by a human, and it is therefore dependent on circumstances in the social world.

2.2 Modified action research strategy

The matters described in the preceding section shape the chosen research strategy. Initially, we did not label the strategy. Only after the studies were carried out, it was found that the strategy employed in some respects resembled what in the methodology literature is referred to as an *action research* strategy. Nevertheless, there are significant differences between the adopted strategy and action research. "Action research aims to contribute both to the practical concerns of people in an immediate problematic situation and to the goals of social science by joint collaboration within a mutually acceptable ethical framework" (Rapoport 1970: 499). An action research strategy is essentially defined by four characteristics; it deals with a (i) practical research problem in a (ii) participatory style. In addition, the pursuit of (iii) change, though a (iv) cyclical research and feedback process, is considered an integral part of research (Denscombe 1998: 57). The following paragraphs briefly examine these defining characteristics in relation to this study:

Practical research problem. In this case, the research is concerned with the problems that organizations face, and the processes they go through, as

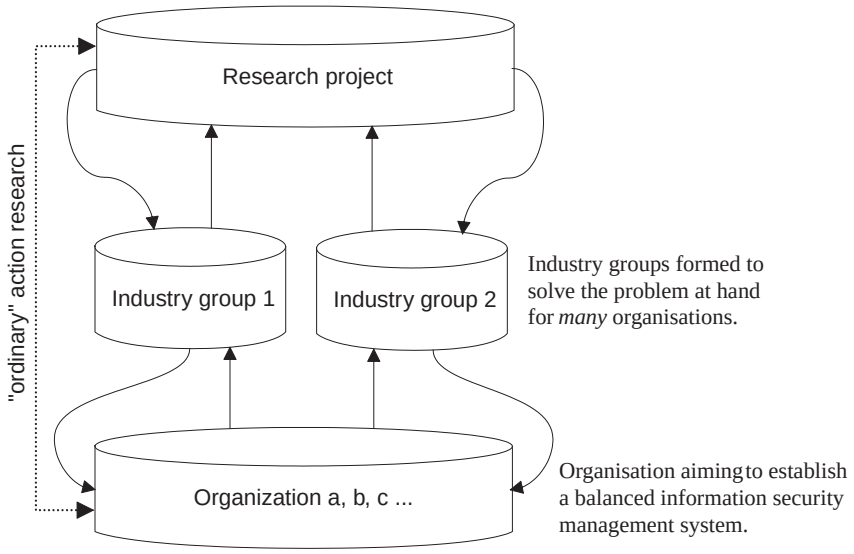


Fig. 2.2: *The difference between the adopted research strategy and familiar action research.*

they are aiming to establish a balanced information security management system. In Sweden, over 40 organizations have formed a group under the Swedish Standards Institute, named Project Information Security Management Systems *TK099*, aiming to work with these issues. As briefly mentioned above, a part of this research was carried out in that context (chapter 5). Another part of this research was done in cooperation with information security experts and the Swedish Information Processing Society (chapter 4) – also this of a direct practical nature. Therefore, the problems under study in this thesis are clearly of a practical character. However, in action research literature it is often assumed that the problem solving and research process takes place *at the level of one organisation*, and that it deals with a problem in that very organisation. This is not the case here, as illustrated figure 2.2. This means that the cycles of information gathering and feedback to/from the key sources - the organisations facing the problems studied - of empirical materials have been *indirect*. Thus, this approach is slightly different than that in "ordinary" action research. This has doubtless affected the research results since some degree of analytical generalisation has already been done by the participants in these two industry groups (figure 2.2). As researchers in these groups, we – and our sources - have been comfortably positioned with some distance from organisations actually facing the problems. That has opened up the possibility to view the world less chaotic and more structured – leaving us with a more idealised view of reality for good and for worse.

Participative. The pilot certification work group is unique in that it brings together certification auditors, information security consultants, government agencies, organisations interested in information security certification and researchers (us). All of these parties have been working together with the aim to

generate and share the knowledge created. The respondents – the practitioners - have shared their own experiences and insights; we have merely summarized them in this study. They needed the knowledge themselves, that is why they decided to participate in the pilot certification group. We have participated in the pilot certification work group during the course of two years. Likewise, the Swedish Information Processing Society and the information security experts, together with whom we developed the evaluation tool and method presented in this thesis, were also participating to learn themselves and to help other organisations in their evaluation efforts.

Change. The third defining characteristic of action research is change, and reflection on the effects of change. Also here, the change instilled is indirect – on the level of the industry groups, so there is very little reflection of the type "did this change do any good in the organisation?", and more of a change and calibration of *views and ideas*. For example, the pilot certification group wanted to reach a common understanding of what is required for the successful implementation and certification of information security management systems according to the 7799 standard – they were seeking a methodology of how this could be done. The parties wanted to change - or calibrate - their views on these issues so as to reach consensus.

Cyclical feedback. The results were (and still are) fed back by means of presentations of what we have learned, and through written feedback reports. There are three target groups for this feedback; the practitioners in the projects (and in the study), the other information security and certification practitioners in Sweden, and the information security community at large – research as well as practice. This thesis is also a part in this cyclical feedback loop.

2.3 Limitations of action research

There are no research strategies without disadvantages – this is also true for action research. The main scientific objection to this kind of research strategy is probably that if can affect the "representativeness of the findings and the extent to which generalizations can be made on the basis of the results" (Denscombe 1998: 65). This is true also for this study, but the objection assumes that the action research project takes place in only one organisation (a "work-site approach"). In contrast, this study is concerned with experiences and insights from *many organisations* and *many different contexts*, which may make the results more universal. Another objection against action research is that the researcher most likely cannot be totally detached and objective in relation to the subjects under study, since s/he is so immersed. This is against the positivistic ideas of research, as pointed out by for example Susman and Evered (1978). However, this fact can also be viewed as a scientific advantage since it gives the researcher a closer and deeper view of what is studied.

2.4 Data collection and analysis methods

The specific research method used - within the defined action research strategy - differs from paper to paper (chapter to chapter) depending on the most suitable method for the problem at hand. Were relevant, each chapter describes the research process, principles and methods of the specific study. Among the data collection methods used are questionnaires, direct observation, participation, and documentary review. Methods for analysis of data applied are different types of qualitative analysis, such as the grounded theory based analysis method offered by the software tool Atlas.ti.

3. THESIS FRAMEWORK

3.1 Framework introduction

Any organization that wants to work systematically with information security will need to go through certain stages in pursuit of the goal of optimised information security. In essence, these resemble the common analytical stages we know from almost any type of ideal organizational- or even software development process:

- It is common to start out with some kind of analysis of where we are today and what we need to do to get where we want to be tomorrow.
- The next step is often to start describing or designing the ideas or solutions that will take us from the current situation to the identified ideal situation.
- Once these ideas or solutions are formed and explicated, they should be put into use in the organisation by some kind of implementation procedure.

As soon as the new ideas are used in the organisation, it is possible to gather information of how it works, with the aim of identifying further room for improvement – a new change cycle can be initiated.

There are many models available – especially within the quality management area – that describe these or comparable stages. For example the PDCA cycle, originally developed by statistician Shewhart and described in the quality management literature by Deming (1989). The PDCA cycle consists of the four stages plan, do, check and act (Deming, 1989):

- *Plan:* Analyse the current situation to identify room for improvement and promising solutions.
- *Do:* Test the solutions in a small scale first in order not to disrupt critical processes.
- *Check:* Find out if the solutions are giving the expected effects, and if they do;
- *Act:* Implement changes on a wider scale.

Models like these let us express the major activities involved from start to finish, or in this case from 'problem faced' to 'problem solved'. The PDCA cycle is often used to describe organisational change processes. Lately, it has often been used – at industry conferences and even in standardisation documents, such as

7799 part 2 under revision (Humphreys 2001) - to portray the activities involved in information security management projects. However, since the PDCA model was developed mainly to cater for the need of a systematic methodology when optimising automated manufacturing processes in the 1950s, it is not very well suited to describe the major activities in the ISMS process. For example, the *plan* stage includes both *analyses* of the current situation as well as *designing solutions*. In information security management, these two are most often rightly seen as two discrete activities. In addition, the *do*, *check*, and *act* stages clearly presume – although not explicitly - that it is possible to implement one small change and then measure the effect of that. This approach will work well for single, continuous improvements in an organisation (in line with the Japanese total quality management philosophy, *Kaizen*[1]). When implementing a new information security management system, however, we are normally attempting to bring more than a few significant changes to the organisation at once. In these cases, we have to wait with the *check* activities until the management system is already brought into play – when we can record feedback information from the ISMS in operation. For this, we need our own PDCA model that is tailor-made for information security management.

The next few sections will describe such a model, including its activities, the associated inputs and outputs, and major issues pertaining to each activity. The model will form the high-level framework for this thesis.

3.2 Proposed ISMS process model

3.2.1 The need for a process model

The international standard for information security management – sometimes called the "ISO9000 for Information Security" – is primarily requirements-oriented, meaning that is states the requirements organisations should satisfy if they want to undergo certification in accordance with the standard (ISO 2000). It requires that the organisation has balanced its information security management system to counter the threats its information assets face. What is not spelled out in the standard though, is *how these requirements can be reached*. Many organisations here in Sweden, and in other countries as well, have been stalled in their plans to adhere to the requirements of the standard, since they simply did not know what steps to take to satisfy those. This was evident for most organisations in the Swedish pilot certification scheme. Although many organisations are hesitating to actual certification, many aspire to adhere to the standard anyway, as it is seen to represent best practice in information security management. By proposing an ISMS process, and describing the activities involved, we take a first step toward resolving the problem depicted above. As always with process models – they can never be applied fully to any real world situation without first adapting it to the context at hand.

[1] The essence of the Japanese quality management philosophy *Kaizen* is to improve an organisation or a process continuously in small incremental steps.

3.2.2 The ISMS process model evolution

This ISMS process model has been developed gradually through participation, observation, and interaction with information security consultants and other individuals working in projects trying to satisfy the requirements of the standard. At times, we have been immersed in one of the stages, and at other times, we have been concerned with the totality of the ISMS process and what it looks like. All organisations have their own methods and views. However, working together with some thirty individuals trying to interpret the standard, after more than two years of discussions and agreements and disagreements, we believe that the ISMS process model presented here is one that many practitioners and academics will subscribe to. The ISMS process model describes the stages and the important activities involved on a level of details still leaving room for situational adaptation.

3.2.3 High level view of the ISMS process model

The model divides the ISMS process into its sub-processes (figure 3.1).

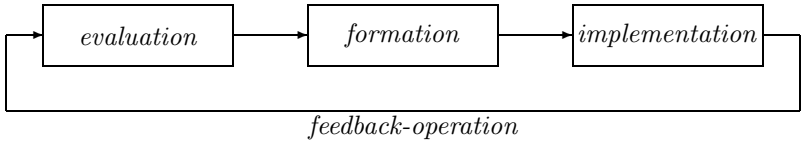


Fig. 3.1: *The Information Security Management Process (ISMS Process).*

The evaluation stage includes everything it takes to assess the current situation vis-à-vis information security management in the organisation. It takes into account not only the administrative / organisational security issues, but also the technical (IT) security issues. The main result (output) of the evaluation stage is reports of vulnerabilities and deficiencies in relation to information security.

The *formation stage* takes these reports as its main input. It also adds knowledge about the organisation, its business processes, culture, etc. The goal is to design and develop solutions tailor-made to the organisation that will remedy any vulnerabilities and deficiencies in the current situation. The formation stage it largely analytical in that these solutions still "on the drawing board".

The *implementation stage* takes the solutions from the conceptual level and makes them work in the organisation. It entails for example installing and configuring technical security mechanisms as well as information security education and training to employees.

Once implemented, the ISMS is in *operation* and it starts to generate feedback information to the next iteration – as input into the new evaluation phase. Now, let us examine each of the stages more closely.

3.3 Evaluation stage

This section aims to discuss and clarify issues pertaining to the evaluation stage of the ISMS process. By doing this, it also lays a foundation for the coming chapters by making explicit answers to questions such as: What is the subject of evaluation? What types of activities are generally associated with an evaluation? What does an evaluation result in?

3.3.1 Unit of evaluation

Information security evaluation methods (or, in same cases, frameworks) can take on many different forms and focus on a range of different aspects: The IT Baseline Protection Manual (BSI 2001), Orion (Fillery-James 1999) and Odessa (Warren *et.al.* 1997) can help evaluating the security of information or IT in an organisation. So can CRAMM (2001) and SBA Scenario (SISP 2001b), but from a strict risk/threat perspective. The SSE-CMM (1999) can help evaluating a developers' systems security engineering capability, and the CEM/CC (NIST Common Criteria Project 1997) the security functionality in (e.g.) an application system. If conducting an evaluation using CobIT (ISACF 1996, 2000), the focus will be on management control over all activities in the IT department – some only indirectly related to information security. Evidently, there are many different security evaluation methods, and all of them have slightly different foci. This thesis has a special kind of evaluation focus in mind in the evaluation stage of the ISMS process. The unit of evaluation under study here is an ISMS and how it works in reality. An ISMS (information security management system) is the organisational infrastructure (it is not a computerized system) that enables information to be shared, whilst ensuring the protection of information and information processing assets (Brewer 2001). It consists of a set of controls such as "policies, practices, procedures, organizational structures and software functions" (SIS 1999a, 7). Although the management system is declared in written documents such as the information security policy, it is not enough to identify and evaluate what is written in these documents. Instead, these written rules describe technical and administrative controls that exist in reality that can - and should – be evaluated.

3.3.2 An overview of the evaluation stage

The goal of the evaluation stage is to assess the current information security situation of the organisation (figure 3.2). This evaluation takes into account not only the administrative / organisational security issues, but also the technical (IT) security issues. Before any fruitful evaluation can take place, we need to gather some information:

Business & IT strategies. All organisations have a strategy, and many have it formally documented. In either case, here we can expect to find information of where the organisation is today (*e.g.* SWOT-analyses) and what it is trying to achieve (*e.g.* business objectives such as market share

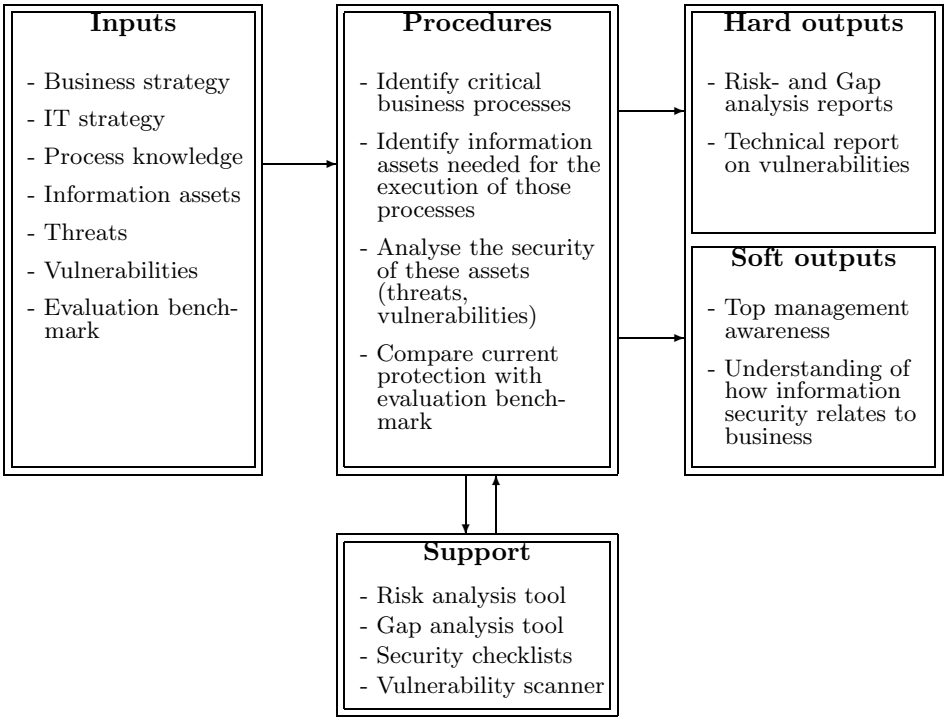


Fig. 3.2: *The evaluation stage*

and profit), and how to get there (*i.e.* the strategy itself). In the evaluation stage we need to analyse both types of strategies (IT and business), so that we can elicit what business processes are critical in relation to the organisations' current strategy and objectives.

Process knowledge. Once the critical processes are identified, we need - as input – information about how these processes work in reality. Again, some organisations will have this formally documented with flowcharts of critical processes and associated activities. Other organisations might not have this documented, so sometimes this has to be done as a part of the evaluation stage. It is important to involve people with good knowledge of the process to be documented.

Information assets. We need to have a grasp of the organisations information assets (*e.g.* Information, databases, application systems, documents, *etc.*). There is no need to list all information assets in the organisation – this would be hundreds of thousands even in small organisations. It is only the information assets that are crucial to the successful execution of the identified critical business processes that should be included in the analysis.

Threats and vulnerabilities. Threats - such as fire, flood, and hackers – against the information assets should be considered. This can be done

using a scenario technique ("What would happen if..."). Known technical vulnerabilities should also be used as input to the evaluation stage.

Evaluation benchmark. We need some reference to evaluate against. When we know where we are today, we also need to be able to compare this to some ideal situation (where we want to be). This evaluation benchmark can be either the current information security rules of the organisation or a collection of best practices for similar organisations.

While describing the inputs, we have also started to express the procedures of the evaluation stage. First, we need to identify critical business processes and identify crucial information assets needed for the execution of those. Then we need to consider the consequences for the organisation if a threat against a certain asset would materialise. In addition, we need to look at the current protection for each asset and compare this with current rules or best practices. To aid in this work we can use a number of support tools such as automated risk- / gap analysis software, security checklists, and (IT) network- / system security scanners. This support tools can help with documenting and reporting findings, as well as automatically search large computer networks for vulnerable IT systems (all tools have serious limitations though).

The result of the evaluation stage is some kind of evaluation documentation, *e.g.* a report showing the result of the risk- / gap analysis efforts and documents showing vulnerabilities found in the current IT-infrastructure. In addition to these "hard" tangible outputs, there are some important intangible or "soft" ones: By communicating the evaluation result to top management, their awareness for information security issues is heightened, and in many cases their support for the information security efforts in the organisation grows stronger. Also, the persons participating in the evaluation gets an understanding of how information security relates to business, as the connection from business objectives and strategy down to protection of information assets is illuminated.

3.4 Formation stage

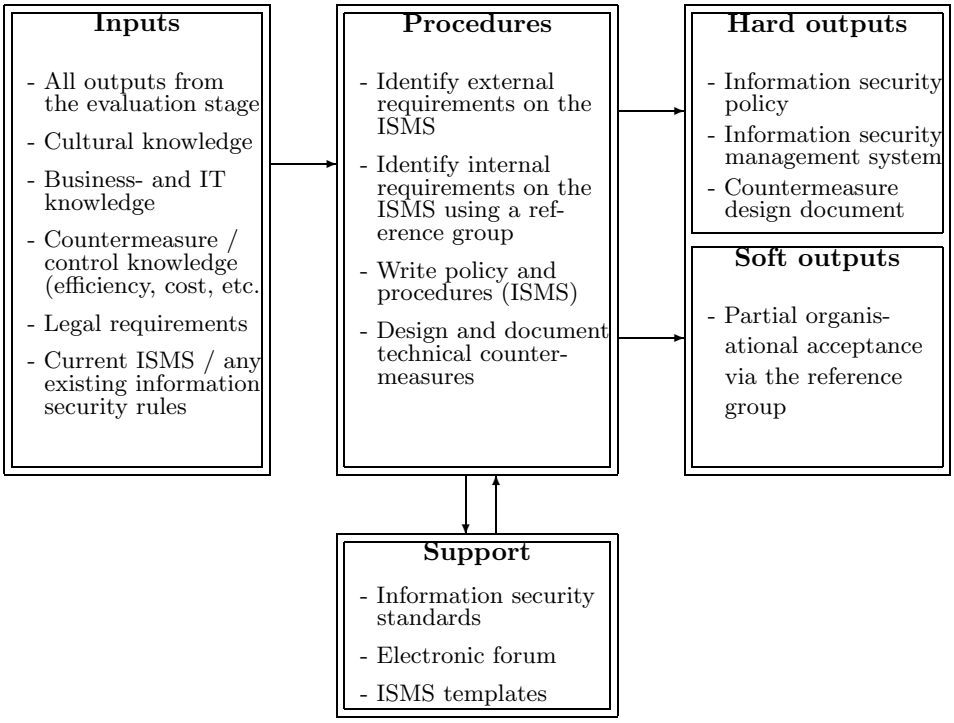


Fig. 3.3: *The formation stage*

The goal of the formation stage is to design a technical and organisational infrastructure for information security that suits the business (figure 3.3). Such an infrastructure is documented as an information security management system – often presented in the form of a security handbook for the organisation. The written documents contain policies, rules and procedures with regards to how employees should handle information securely. In addition to rules aimed at humans, there is a need to create rules for many IT-systems, *e.g.* "Only allow access from computer X" or "Require that all users change passwords within a 42 day cycle". In the formation stage, we only design the solutions – they are still only on the drawing board and not in the reality (that is for the next stage).

When forming the ISMS, we need information from different sources, so that we can create an ISMS that is suitable for the organisation:

Risk- / Gap-analysis reports, Technical security reports These documents gives us a view of the current state of information security, so that we know what we already have and were we start from.

Cultural, business and IT knowledge The existing corporate culture can either enhance or hinder our efforts. Therefore we must have an idea of

what it is like, *e.g.* what kind of behaviour is generally viewed as "ok" in the organisation. We also need knowledge of restrictions and requirement from the business and the current IT-infrastructure. *E.g.* Some parts of the organisation might require tighter security then others, and the current IT-infrastructure might set limitations to what we can do in terms of network security.

Countermeasure / control knowledge We need to know; what is available, to what cost, and what will it do for us? Countermeasures range from technical controls such as firewalls and access control- and intrusion detection systems to information classification rules.

Legal requirements Most countries have a data protection act, a legal framework for corporate governance (for financial accounting, etc.), and so on. Relevant laws have to be identified and the requirements on the ISMS from each law have to be taken into account.

Current ISMS / existing information security rules If the organisation already have rules about information and IT-security, these have to be taken into consideration too, as they are the formal point of departure for the new ISMS.

Some of this information will be found in secondary sources like reports and existing policies, but most information will have to be brought into the formation stage thorough the involvement of people with that knowledge. Once we have the information at hand, we can list all the external and internal requirements on the ISMS, and then start to write the documents and design the technical controls deemed cost effective or required for other reasons. While doing this, it is helpful to have help from information security standards and templates, as they often include ideas of common countermeasures. If the project involves many persons or if the geographic distribution of the persons involved is wide, then it might be a good idea to do some of the discussions via an electronic forum, especially set up for the project.

The result of the formation stage is a security handbook consisting of the information security policy and all rules and procedures, as well as a documentation of the chosen technical controls. The formation stage should be carried out using a reference group of persons from different parts of the organisation, because their knowledge is needed, and also because that is a part of the process of gaining acceptance for the ISMS in different parts of the organisation.

3.5 Implementation stage

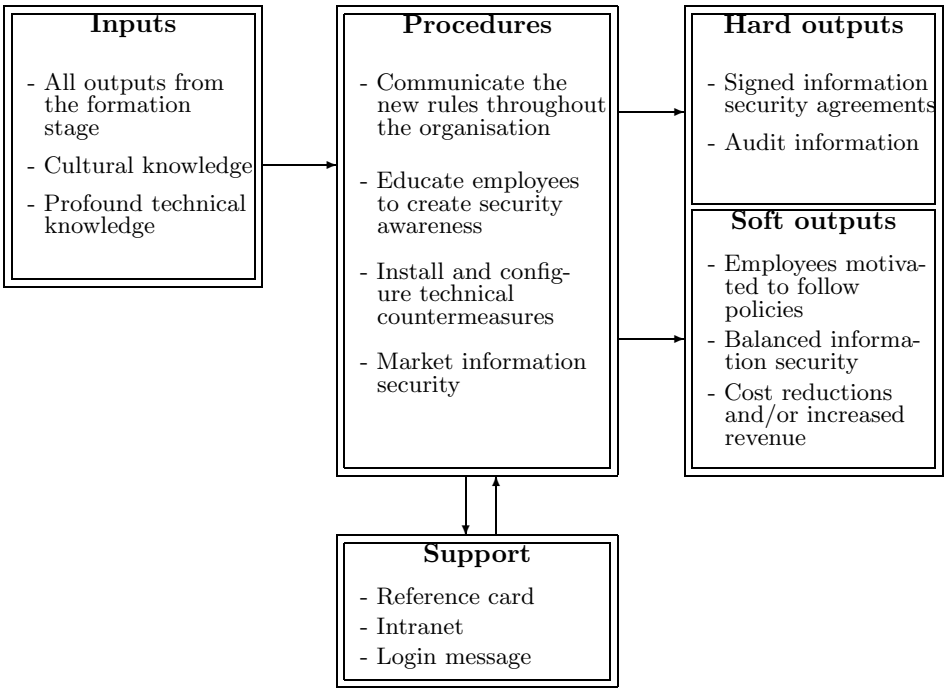
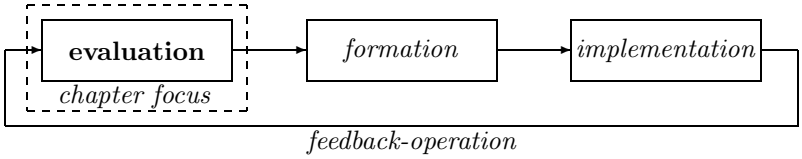


Fig. 3.4: *The implementation stage*

The goal of the implementation stage is to take the ISMS, including also the technical controls, from the drawing board to reality(figure 3.4). This is the most difficult of all the stages, and it is also here that it will be evident if the other stages – the evaluation and formation stages – were carried out properly. The rules in the ISMS have to be communicated to relevant groups throughout the organisation, employees have to be motivated and educated and trained in using new technical security controls and following the rules agreed in the ISMS. Also, all the IT-related solutions have to be installed or (re-)configured. Information security has to be marketed so that the organisation accepts to follow the rules laid out in the ISMS. This work can be aided by using a reference card or a brochure communicating the most important rules and explaining the most common technical controls (*e.g.* "This is how you use the anti-virus application"). If all goes well, the employees will sign off on and feel motivated to follow the rules in the ISMS. In that case, the result is that the organisation will have reduced the cost from security breaches and in some cases even enabled new streams of revenue in the future.


evaluation
formation
implementation
chapter focus
feedback-operation

4. EVALUATION STAGE – PAPER A: "INFOSECURITY ASSESSMENT USING SBA CHECK"

This chapter describes an approach for evaluating information security in organisations. The presentation is divided into one section on the software tool, and another on the method that can be employed when using the tool in conducting an evaluation[1]*. It should be noted that the type of evaluation proposed here is not the only kind of evaluation that needs to be done to get the full view on the information security situation in organisations. An example is the need for deeper analysis and evaluation of the security of critical IT systems that would not be completely covered by this approach.*

4.1 The software tool

4.1.1 Introducing SBA Check

SBA Check is a software application package, which is aimed at supporting the evaluation of information security in organisations. As the name of the software tool indicates, it is a checklist-based approach to evaluation. This means that the evaluator(s) are guided through the whole evaluation process by means of searching for information and answering questions asked by the software tool with regards to the information security measures (controls) in the organisation (figure 4.1).

In addition to guiding the evaluator through an evaluation, the tool helps to document the information security situation in a systematic fashion. For example, information regarding the current situation, potential improvements, assessment, any identified deficiencies, for each security control present in the used checklist can be documented. The evaluator can learn how other organisations have solved similar security problems by turning their attention to the 'best practices' database in the tool. One of the main ideas with this kind of tool is to enable the automatic generation of relevant reports to different stakeholders (figure 4.2). For example, graphical reports including descriptive statistics for top management, and detailed reports for IT professionals responsible for

[1] This chapter is based on a previously published research paper (Björck 2000). The original title of the paper was "Auditing Information Security Management Systems - Towards a Practical Method"

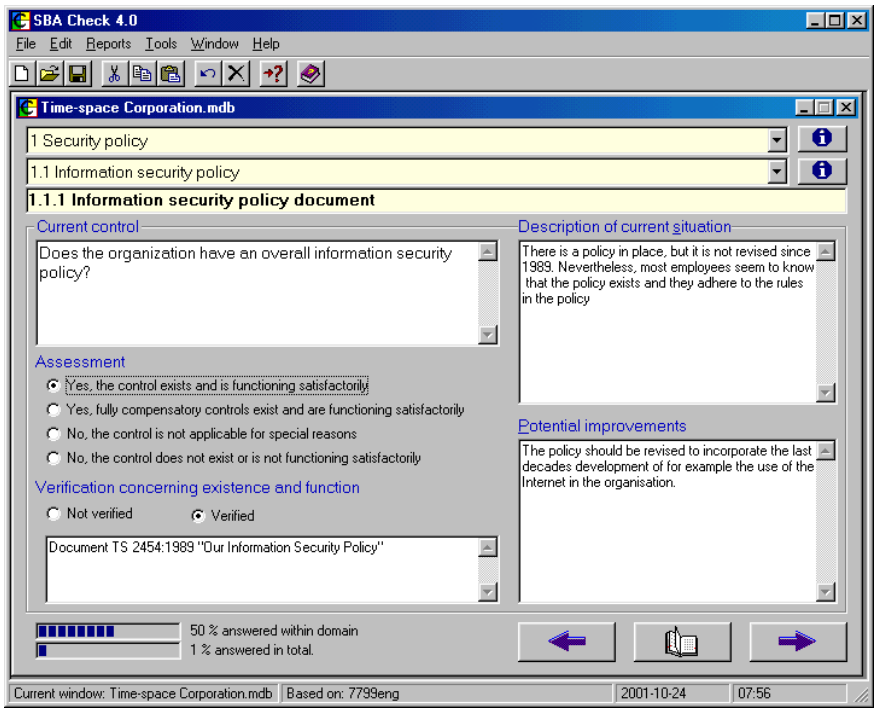


Fig. 4.1: *SBA Check main evaluation interface.*

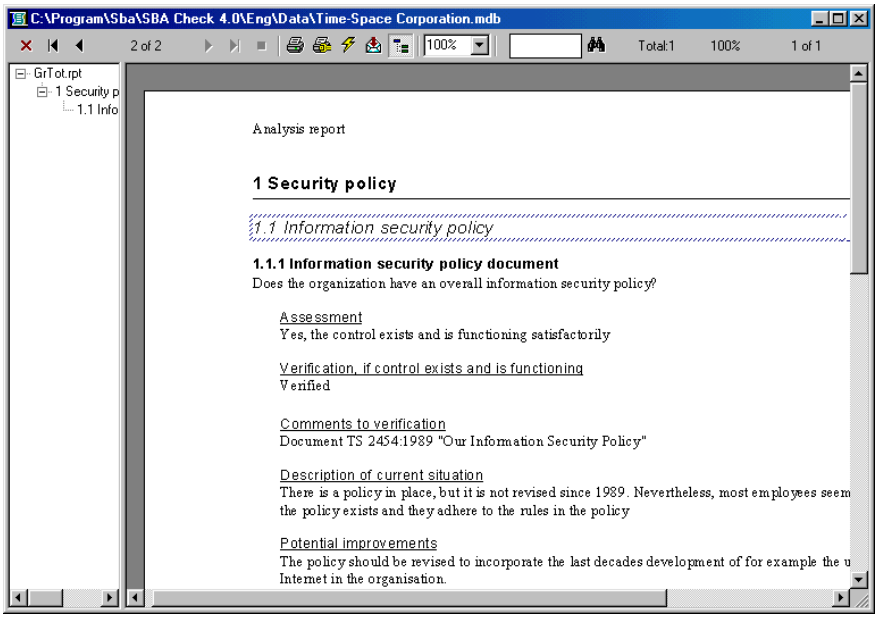


Fig. 4.2: *SBA Check report example.*

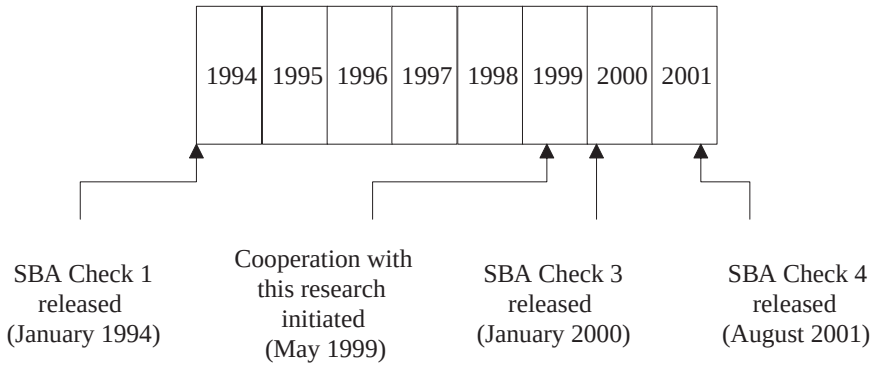


Fig. 4.3: *Historical development of SBA Check.*

developing and implementing solutions to resolve identified vulnerabilities and deficiencies are available.

4.1.2 Historic development of SBA Check

The Swedish Information Processing Society (SIPS) first released a tool called SBA Check in 1994[2]. This was never widely used since it was not perceived to be very user friendly, even though it was excellent in theory. This version – 1 – focused on *IT systems security*, so it was a totally different tool than the current version. In 1999, SIPS had plans to revise the tool, and this is where we joined the development of SBA Check (figure 4.3). The result of the revision process was a totally different tool now focusing on information security in organisations. The first version – called version 3 – came out on January 20, 2000. The current version, as of December 2001, of SBA Check is 4.1. In terms of basic functionality, it is almost identical to version 3, even though some features have been added. One of the main improvements is that the tool is available in English now.

4.1.3 This research's contribution to the development of SBA Check

As the owner of the SBA Methods, the Swedish Information Processing Society initiated, financed and supervised the revision of SBA Check. Many organisations and individuals were involved in the process – from initial ideas, via requirements specifications and programming, to testing and later marketing. As the only academic representative in this group of information security experts and system developers, we assumed a key role in the development of SBA Check. Our specific contribution was the:

[2] Please note that SBA Check is one tool in a set of tools and methods marketed by the Swedish Information Processing Society, the latter often referred to as the 'SBA Method'. 'SBA' stands for 'SårBarhetsAnalys', the Swedish term for vulnerability analysis, and was originated in the early 1980s. Another related and well-known tool and method in the same family is that for risk analysis called 'SBA Scenario'.

- Formulation of the working evaluation principles on which the tool is currently based and presenting these by means of a first version of the main user interface, and primitive working prototype (see appendix D for details)

- Crafting of the requirement specification for the content of the tool, to be followed by content deliverers and the programmers.

- Development and documentation of a methodology for the evaluation process. This methodology is made explicit later in this chapter.

SBA Check was created as a true team effort, and there were many other activities in the development of the software tool that is not listed here.

4.2 The evaluation approach

4.2.1 Introduction to the evaluation approach

The evaluation approach presented here can be employed, together with the methodology software tool *SBA Check*, for information security management assessment in organisations. The focus in this type of evaluation is parts of the organisational management system for information security, such as information security related policies and –procedures. Critical technical security mechanisms are also assessed.

The philosophy behind the SBA Check tool and this approach is *simplicity* and *efficiency*. The software tool will guide the user through the evaluation by asking a set of bespoke questions, each representing potential information security controls (countermeasures). The approach results in a snapshot view with regards to the information security situation in the analysed organisation. This approach also helps identify possible changes that would help reduce or eliminate identified weaknesses.

The difference between this approach and classical risk analysis is that in risk analysis the starting point is to identify *threat scenarios* that can negatively affect information assets. Then one tries to establish the probability for a scenario to materialise and its possible consequences in monetary terms. Once this is done countermeasures are identified to reduce the identified risk. Using the approach presented here, the starting point is diametrically opposite – it starts with a list of countermeasures (referred to as "controls") that are generally accepted as best practice, and thus suitable for most organisations. By matching these controls against the organisations business needs and requirements, we end up with a faster and more efficient evaluation approach. However, there are application areas where a classical risk analysis can be fruitfully used also within information security, but problems with *e.g. monetarizing risk* and *pricing information assets* and *discounting monetary flows to net present values* are often too great to make it a worthwhile exercise.

4.2.2 Overview of the approach

The evaluation approach entails three stages (figure 4.4):

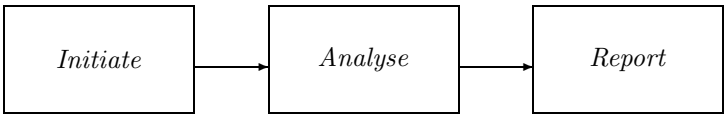


Fig. 4.4: *Overview of the evaluation process.*

1. *Initiate*: Set-up the evaluation
2. *Analyse*: Gather information and perform evaluation
3. *Report*: Communicate the findings

The following sections will describe each of these stages in turn, and conclude with a discussion about the presented evaluation approach and the associated software tool.

4.2.3 Stage 1: Initiate

Objective: To build a solid foundation for the evaluation process resulting in a documented evaluation plan and –agreement. Figure 4.5 shows an overview of the initiation stage.

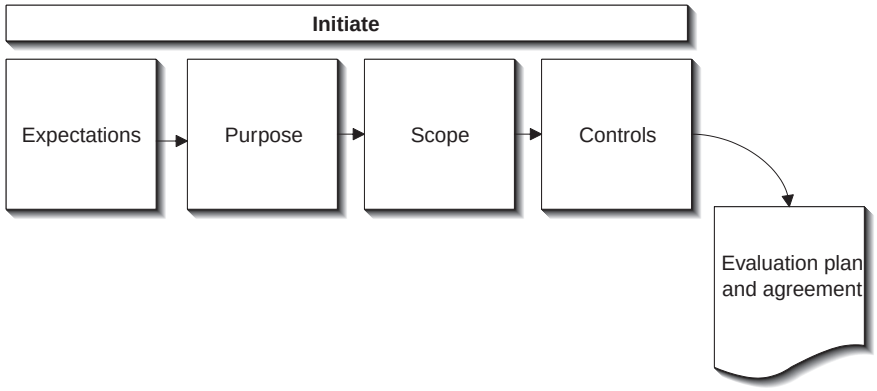


Fig. 4.5: *Overview of the initiation stage.*

Fig. 4.6: *Example of expectations on the evaluation.*

Expectations

One of the most important issues is to identify stakeholders' (client or other benefactor) expectations with regards to the evaluation results as early and accurately as possible. By identifying and co-developing these expectations at the onset of the evaluation, the result is more likely to be perceived as valuable and useful. The ideal method for identifying and co-developing expectations differs from situation to situation. However, a meeting in person with important stakeholders to discuss the impending evaluation has proved to be a very efficient way to clear out any misunderstandings and to identify and discuss any implicit and explicit expectations. Expectations can relate to all aspects of the evaluation (figure 4.6).

Action point: Stakeholder expectations should if possible be agreed on and documented in the evaluation plan and agreement.

Purpose

The purpose of the evaluation should also be established at an early stage, since this will determine how the evaluation ideally should be conducted. The core questions here are:

- *Who* will be the recipient(s) of the evaluation results?
- *How* and for *what*, are they planning to use the findings?

Information gathered and analysed in the evaluation process must be in line with the overall purpose of the evaluation. For instance, the purpose governs

the required accuracy and precision with which the questions ideally should be answered, and if any kind of verification is required or not.

Example; *purpose* and *implications* for the evaluation process:

- A client asks for an SBA Check evaluation of the information security situation in the organisation.
- The purpose is to *identify current deficiencies* and to *pinpoint solutions* that could be implemented to solve these deficiencies.
- Therefore, potential improvements will have to be documented with extra details, so that the evaluation result can be used as input in the decision situation when the client is going to decide on which countermeasures to implement.

Action point: Document the purpose of the evaluation in the evaluation plan and agreement.

Scope

The scope of the evaluation should be established to ensure that the evaluation really analyses the decided unit-of-analysis. This is especially crucial if the evaluation result is to be used as a basis for certification according to some information security standard, such as ISO/IEC 17799 (ISO 2000). Some common delimitations of scope include:

- Which IT-systems and communication networks should be included in the evaluation? (Only those in-house or also outsourced?)
- Which parts of the organisation should be included in the evaluation? (Which geographical, juridical, or functional units? Only the head office? Subsidiaries?)

In large organisations, for example, it is common to conduct multiple small evaluations on organisational units and then compile the findings.

Action point: Document the scope of the evaluation in the evaluation plan and agreement.

Controls

The final activity of the initiation stage is to establish the *set of controls* to perform the evaluation against. The choice of controls depends on all of the three previous activities (expectations, purpose and scope). This is essentially choosing which checklist to use for the evaluation at hand. SBA Check is delivered with three sets of controls:

- Check

- ISO/IEC 17799
- FA22

In short, *Check* was developed by the Swedish Information processing Society via leading information security experts in Sweden, ISO/IEC 17799 contains all the controls listed in the international standard, and FA 22 contains all controls related to the rules about computer systems security as stated in the Swedish regulation *Beredskapsförordningen* clause 22. This regulation is only applicable to society-critical systems, but may still be of interest for some evaluators.

Most evaluators are likely to choose to evaluate against either the '*check'* set of controls or ISO/IEC 17799, as they represent Swedish and international "best practice" (respectively) for information security management. However, it is also possible to adopt a different set of controls to evaluate against, as there is support for this in the SBA Check software.

Action point: Record the choice of controls in the evaluation plan and agreement.

Evaluation plan and agreement

Stakeholders' expectations, evaluation purpose and scope, and the selection of controls are now established. All of these should be documented in an evaluation plan and –agreement (Figure 4.7). The objective with such a document is:

- To ensure that stakeholders' have a good grasp of what they can expect with regards to the evaluation results,
- To ensure that all individuals involved in the evaluation in any way understand its purpose and scope if required,
- To help the evaluator to focus on the agreed scope during the evaluation process, and
- To aid the evaluator and stakeholders' recollections in any discussions and potential future disagreements about the evaluation after it has taken place.

4.2.4 Stage 2: Analyse

Objective: To gather and analyse information about the information security situation under examination, aiming t o arrive at a truthful view on the situation. This stage, as described here (figure 4.8), is to be executed once for each question (representing a control).

Examine question to determine evaluation strategy / Identify information sources: The first step is to read and understand the question asked by SBA Check. To further explore the meaning of the question, one can refer to the "best practice" description for each question. The nature of the question

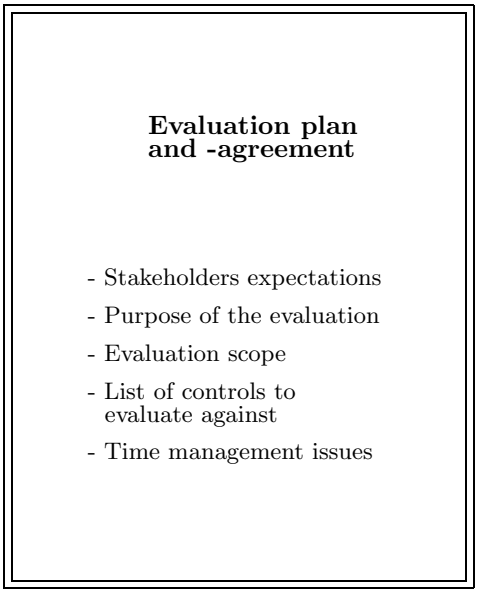


Fig. 4.7: *Typical contents of an evaluation plan and –agreement.*

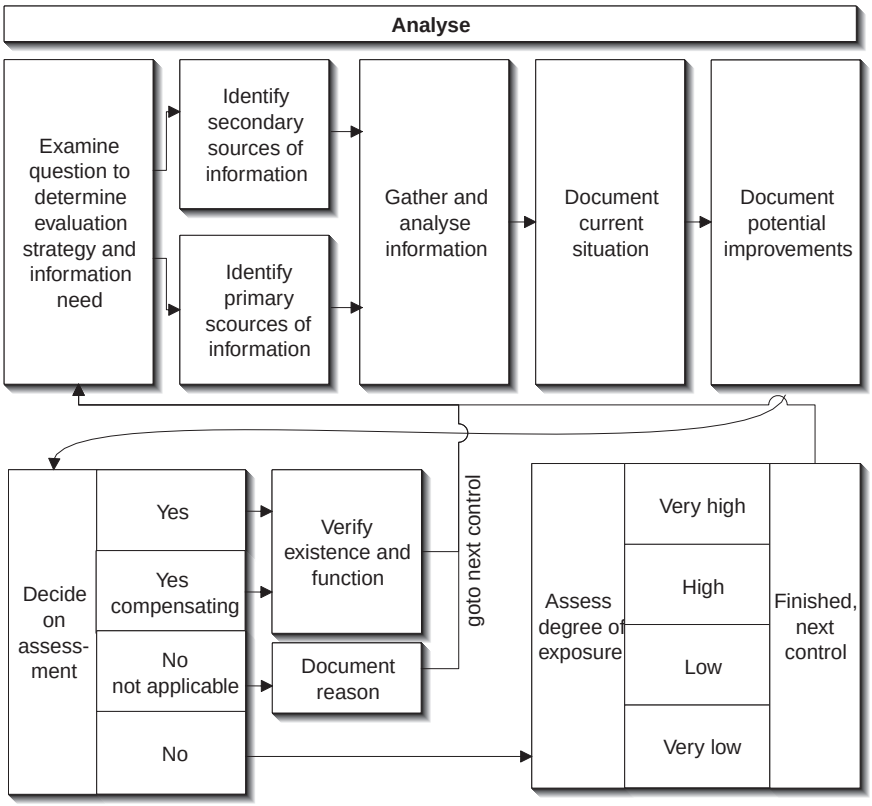


Fig. 4.8: *Analysis stage.*

determines the ideal evaluation strategy, and the information sources needed for the evaluation. For example, if the question is regarding a technical control, one might have to consult system utilities to gather information from IT-systems. If the question is regarding the existence and function of some formal procedure, one might have to consult the organisations' security handbook and interview those supposed to carry out that procedure.

Gather and analyse information: This stage can be very complex if dealing with a large or geographically dispersed organisation, or if the IT-systems are very complex and heterogonous. Sampling is often necessary as it is not economically feasible to for example interview all users about their awareness of the information security policy.

Document current situation / Document potential improvements: Once information is gathered and analysed, the current situation with regards to the control at hand can be documented in the software tool. Details of the current situation might include for example references to existing information security documents and results of interviews. Potential improvements can be based on either the evaluators' direct knowledge or be inspired by the best practices described in the tool.

Decide on assessment: There are four possible quantitative alternatives:

- *Yes*, control exists and functions adequately
- *Yes*, compensating control exists and functions adequately
- *No*, control not applicable for special reason
- *No*, control does not exist or does not function adequately

What is adequate is a multi-dimensional judgment – it depends on the organisation's business, its reliance on information and IT systems, and the perceived efficiency (costs and benefits) of the installed control.

Verify existence and function: If one of the first two alternatives is chosen, one can optionally document if any verification of this has been done, such as a real technical test or if the assessment is based on for example hearsay.

Document reason for non-applicability: If the third alternative is chosen – "No, control not applicable for special reason", then this reason must be documented. For example, a question about a firewall protecting the organisation from threats via the Internet might not be applicable to organisations and systems that are not connected to the Internet at all.

Assess degree of exposure: If the forth alternative is chosen, it means that some kind of weakness is identified. In these cases, one can assess the degree of exposure on a scale ranging from "very low" via "low" and "high" to "very high".

Finished: This was the whole process for each control, so now one can start over again with the next control in line. An average evaluation contains circa 100 or so controls, depending on the established set of controls to evaluate against.

4.2.5 Stage 3: Report

One of the ideas behind a tool like SBA Check is the capability of automatic reporting at the end of the evaluation. The report generator can sort the evaluation result according to any criteria, including degree of exposure (to see the vulnerabilities with very high risk first), assessment decision (to see e.g. all controls that failed at all). In addition, graphical report can be generated with statistics of how the organisation is doing in different areas of information security.

It is imperative to communicate the finding in person to evaluation stakeholders, and also to think about the need to keep evaluation results confidential were required.

4.2.6 Discussion and limitations

The tool and methodology's role in this research

At this state, SBA Check and the evaluation approach presented in this chapter can be seen as hypotheses. So far, we have not formally evaluated the use of SBA Check. This should therefore be viewed as one way of conducting this type of evaluation.

Evaluation of the evaluation tool and approach

The formal evaluation from a user perspective of the tool is in the design-phase right now. This evaluation will be carried out be means of a survey of all licensed users of the tool. However, the tool is *informally* tested in two ways already:

1. At courses held by the author of this thesis for information security managers: Circa 100 information security managers and consultants have been attending 2-day courses about the proposed tool and its practical use. The whole course was designed and carried out by the author of this thesis. Each *course* was evaluated using surveys, and the results were very good. In the last course held, 100% or the participants commented on the course as "good" or "very good". Although this evaluation was not about the evaluation approach directly, it can be seen as indicative of the value of the approach since the course was focusing on this.
2. At real evaluations in Swedish and International organisations: Circa 200 licensed users of SBA Check use the tool to evaluate the information security in organisations. Again, this does not mean that the method and tool is good, but it is at least an indication that organisations are eager to use it.

Limitations to the tool and evaluation approach

When choosing to evaluate information security in one way that choice also means other ways are *not* chosen. Each software tool and approaches to evalu-

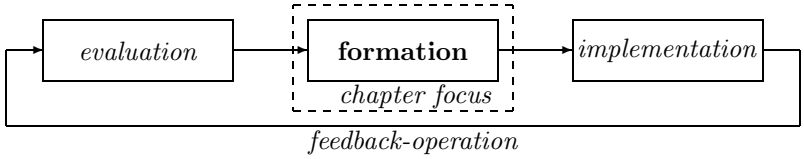
ation has its benefits, but also its negative sides. These are the most important limitations of this approach:

Cost-benefit analysis not supported. In SBA Check, monetary values are left out, so there is no way to analyse the potential costs and benefits of an existing or suggested information security control. As an alternative, the decision of judging a control as adequate or not entails considering the financial impacts on a high-level.

Checklist-based approach. Approaches based on formalized checklists are often, and rightly so, criticized for the inflexibility and rigidity inherent in the approach. For example, a risk or a threat scenario that would require some security measures to be considered that is not included in the set of controls listed in the checklist (or in the evaluation database as in SBA Check) can not be identified and dealt with. Therefore serious threats, critics argue, might be overlooked. This is one major weakness of SBA Check and the evaluation approach described here. The minimize the effect of this weakness, we have taken the following measures:

- *A variety of checklists*: Three different checklists are included in SBA Check, each of which is tailor-made for a specific purpose (for example, one for information security management evaluations and one more focused on IT systems security)
- *Open structure*: Third party developers can develop and market checklists for specific purposes (*e.g.* A specific Windows XP checklist could be used for security evaluation of an XP based computer network)
- *End-user flexibility*: Each user can, via an editor built into the software tool, amend the checklists to suit their environment, organisations, culture, legal system, IT infrastructure, *etc.*

In this way, we have at least reduced the effects of these serious weaknesses of checklist-based approaches.


evaluation
formation
implementation
chapter focus
feedback-operation

5. FORMATION STAGE - PAPER B: "CREATING ISMS - A STUDY OF SUCCESS FACTORS"

This paper presents the findings of an empirical study of certification auditors' and information security consultants' experiences and insights concerning the formation and certification of information security management systems [1]*. Using an action research inspired strategy and a grounded theory like research method, the study describes these particular experiences and insights primarily in terms of success factors vital to the formation and certification processes. Two tentative theoretical frameworks, providing synthesized views of these factors, are put forth.*

5.1 Introduction

5.1.1 Related work

Formation and certification of ISMS (information security management systems) currently interests many researchers and practitioners. Especially 7799 – the British and now also international standard for ISMS (ISO 2000, BSI 1999) - have received a lot of attention in the information security research community lately:

Siponen (2001) criticises 7799, and other information security (management) standards, from the viewpoint of philosophy of science and argues that these standards are were developed based on personal observations that were not scientifically justified. In addition, Siponen argues, the standards in question claim to be universally valid, although they are not.

Eloff and S. Von Solms (1998, 2000a, 2000b) suggests that both IT product security (measured by for example Common Criteria) as well as procedural information security (measured against for example 7799) have to be taken into account when measuring the level of information security in an organisation.

S. Von Solms (2000) declares that information security must be managed on both a macro and a micro level. The macro level (information security at an

[1] This chapter is based on a previously published research paper (Björck 2001). The original title of the paper was "Implementing Information Security Management Systems - An Empirical Study of Critical Success Factors"

inter-organizational level) should be managed with the help of, and measured against, an internationally accepted framework, such as the 7799 standard. The micro level (information security at the intra-organizational level) should be managed through a dynamic measurement system. Furthermore, he argues that an information security certification scheme, such as those set up for 7799, should play an important role in the future.

R. Von Solms makes a business case for the standard using a metaphor of driving a car:

> "Any motor vehicle on a public road requires a valid roadworthy certificate that will indicate that all technical safety and security mechanisms and features on the vehicle are present and functioning properly. The driver needs a driving licence that will indicate that he/she has learned how to drive the vehicle in a secure way by using the technical safety features correctly and effectively. Further, a third party, i.e. traffic officers, will continuously ensure that the vehicle is functioning technically well and also that the driver obeys all road usage regulations." (R. Von Solms, 1999)

He concludes, "... BS7799 can certainly provide the basis to ensure "safe driving on the information super highway" (R. Von Solms, 1999).

Labuschagne (2001) asserts that 7799 could rightfully be used as one of the cornerstones of web assurance in an electronic commerce context.

5.1.2 Justification for an empirical study

Although much has been written about the standard itself, very little has been written about the *practical application* of the standard. And so far, we have not found any published empirical studies on this subject – at least not related to the 7799 standard. Consequently, even though this study is somewhat limited in its scope and depth, it might still prove interesting for practitioner and academics.

5.1.3 Research question

The research question of this study is:

> *What are the success factors to consider while creating a management system for information security?*

5.2 Research method

5.2.1 Research strategy

The high-level research strategy within which this study was carried out can be labelled a modified action research strategy. This strategy is portrayed, and the *rationale* for choosing it is explained, in chapter 2 of this thesis.

5.2.2 Data collection method

Two sets of questionnaires were developed and sent to the respondents. They were composed of open-ended questions, so as to not restrain the thinking of the respondents. Each form contained six questions, and they were slightly different for certification auditors and information security consultants. This paper only report the findings of one question, which was posed in exactly the same wording to both groups[2]:

> *In your opinion, which are the critical success factors for a successful implementation of an information security management system, ISMS? (Please give reasons for your answer)*

Let us comment briefly on three aspects with regards to the wording of the question above:

- The questionnaires were written in Swedish, so this is a translation.
- Although the question does not explicitly refer to the standard as such and to the problems associated with the certification process, the respondents rightly read this into the question because of the context within which it was asked. That context is; that they were asked about their experiences and insights as members of the Swedish 7799 pilot certification group.
- The question uses the term implementation in a broad sense, which differs somewhat from the meaning we give to the term in the ISMS framework in this thesis (in chapter 3). Here, the term encompasses all of the activities in the ISMS framework, while the *focus is on the formation stage*. The reason for writing this explicitly here is only to clarify why the question in this chapter reads "implementation", while the results of the collected materials, and most of this chapter, is focusing on problems and success factors related the creation of management systems for information security (*i.e.* the formation stage).

In total, there are 8 certification auditors and 18 information security consultants in the Swedish 7799 pilot certification group, which makes up the total population. All of these were asked to complete the questionnaire, so we did not need to make a random sampling in this case. The response rate for the certification auditors were 75% (*(6/8)*100*), and for the consultants 72% (*(13/18)*100*). We have not formally analysed why some decided not to answer the survey. However, we do know that most of the ones who have not answered are new members of the group. Being new, they are likely to have limited experience and insights about the exact question. This fact might explain why they did not answer.

5.2.3 Data analysis method

The data analysis method employed is inspired by the ideas of Glaser (1978, 1992, 1998) and his view of grounded theory. However, one significant difference

[2] The two original reports of this study, which reports on *all six questions* is available in Swedish, and included as appendices B and C.

between the adopted data collection and analysis method and the Glaserian view of grounded theory is that we have not employed theoretical sampling (meaning to let initial findings in collected data direct further data collection), since the data was collected in one go using questionnaires.

The answers were ranging from single sentences to quite extensive explanations. The exact answers were imported into ATLAS/ti – a methodology support tool for qualitative analysis of data especially supporting qualitative data analysis. In line with the ideas of grounded theory, analysis was conducted without any pre-determined categories.

First, each answer, for example a sentence, was coded with a code describing its content. Second, patterns were looked for in the data material by comparing the codes from the first stage. These patterns gave rise to new codes, or in these cases categories.

Figure 5.1 illustrates the codes and categories found when analysing the empirical material gathered from the information security consultants. Each individual quote behind each code is *not* shown here. Instead, there is a number in each box indicating the amount of quotes supporting (or rather"forming") each code/category (figure 5.1).

Categories were created based on the following criteria (Guba, 1978):

- *Internal convergence*; codes grouped in a more general category should be semantically related to each other.
- *External divergence*; categories formed should be semantically separate from each other.

Of course, the researchers pre-understanding of the phenomena will affect the process and the result of data analysis. However, this would have been no different even if there would have had been pre-determined categories in the data analysis phase.

The answers from the auditors and the consultants were analysed separately, and therefore they will also be presented separately in this paper. The idea with this was to see if there were any differences in insights and experiences (and views) between these two groups.

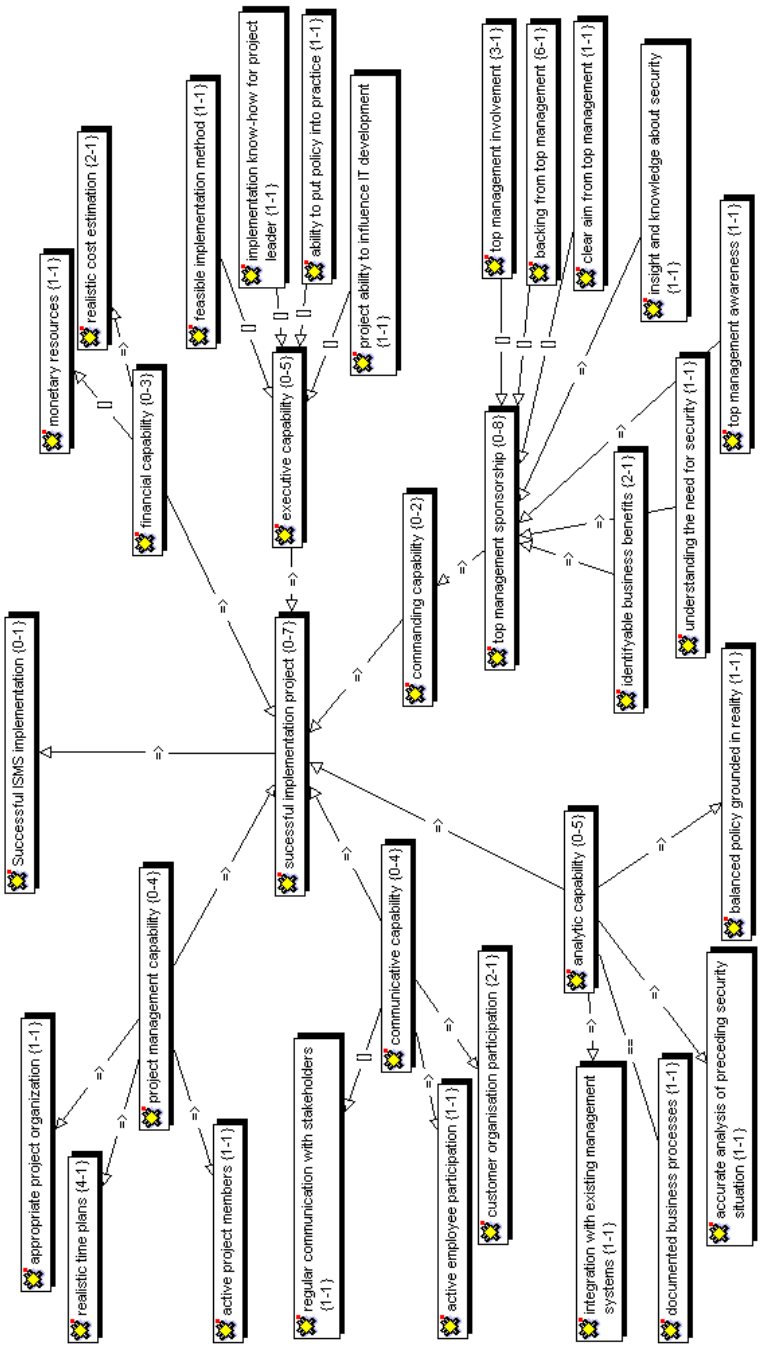


Fig. 5.1: *Illustration of how the empirical materials from the consultants are conceptually generalised – from single quotes via codes to categories - to form the theoretical framework - the sucess factors.*

5.3 Certification auditors' perspective on formation and certification of ISMS

Once again, the question was stated as follows (translation from Swedish to English):

> *In your opinion, which are the critical success factors for a successful implementation of an information security management system, ISMS? (Please give reasons for your answer)*

From the answers, we could distinguish six different success factors. Since the consensus was so profound, we chose to present the answers sorted after each factor- starting with the most important, or at least the most frequently mentioned factor. All the answers fell within these six categories. The success factors for formation and certification, from the perspective of the certification auditors were the following:

5.3.1 Management commitment

Support from the top management of the organization, and their commitment to and understanding of the problems of information security was seen as one of the most important success factors for an efficient formation of ISMS. This factor was mentioned firstly by all of the respondents in this group (auditors), even though there were no fixed answer alternatives and despite the fact that the respondents were unaware of each other's answers. The following quotations speak for themselves:

> *"Top management's interest and commitment in its own ISMS project. . . . "*
>
> *"Top management's commitment and an understanding that the management system for information security must cover the whole business."*
>
> *"Top management's commitment . . . "*
>
> *"Top management's understanding and commitment, in deciding the security policy / security level and to participate actively in the risk analysis and the continuity planning."*
>
> *"Top management's commitment. . . . "*
>
> *"Endorsement from the company's / organization's top management. . . . "*

5.3.2 Well-structured project

Another important success factor, which was identified, was that the ISMS formation project in the organization is well planned and –structured. The respondents expressed it like this:

> *"An organizational unit responsible for the totality and for the risk analysis which is the foundation for all activities. ..."*
>
> *"... a well defined project with delimited sub-projects. ..."*
>
> *"A well developed project plan and a correctly dimensioned project organization. ..."*

Taken together, there are many aspects concerning the organization of the ISMS development and implementation that are mentioned:

- that the responsibility for the project is defined,
- that it is clear who shall carry out the different steps in the project
- that goals, resources and the time plan for the project are developed and documented in a project description, and
- that the resources in the project are well balanced.

5.3.3 Holistic approach

The project members – and other employees – ability to see the "full picture" is stressed by many of the respondents as an important success factor. Sometimes, it seems like the certification auditors have a feeling that the IT-technical aspects are handled in a very detailed way, but at the price to the detriment of obtaining a holistic view. Therefore, they meant that a more holistic approach and thinking in the projects should lead to positive consequences and pave the way to a more successful formation and possibly certification of ISMS. Two of the respondents put it this way:

> *"... that the participants in the work with identifying the risks are representing the whole business, that is not only security but also other parts of the business."*
>
> *"Understanding that the management system for information security must cover the whole enterprise."*

As can be seen from the quotations, it is mainly the connection between the information security and the organizations core activities (processes) that is seen as important – that the ISMS does take into account and that it covers the whole organization – so that the ISMS does not end at the security- or IT department.

5.3.4 Appreciating the need for information security

That the organizations understand the need for information security is another success factor that was identified:

> *"... that the company becomes aware of a need to protect its own, its customers and other stakeholders information."*
>
> *"... understanding that the management system for information security must cover the whole organization"*
>
> *"management's understanding..."*

Although this factor may seem trivial, it is mentioned many times by the respondents. They sometimes perceive a lack of appreciation of the importance of information security from parts of the organization.

5.3.5 Motivated employees

Some of the answers focused on the need to motivate employees:

> *"To motivate the employees to develop processes and procedures within their own areas of responsibility...."*
>
> *"...motivated project management /-participants...."*

The answers focus on the motivation of individuals participating in the ISMS project, such as project participants, project managers, and those responsible for different areas in the organization. After the development of the ISMS, it will also have to be implemented, and at that stage the importance of this success factor grow – at that time, all employees in the whole organization will have to be motivated to adhere to the rules. Further, they should regularly use the technical solutions that the projects have developed and the management decided on – they need motivation.

5.3.6 Access to external competence

The final success factor identified by the questionnaires was the importance of being able to call for external competence when needed:

> *"...good reference persons (preferably certification authorities from the beginning)."*
>
> *"... access to external specialist competence."*

This factor is concerned with both experts and advisors in IT- and information security, but also about opening the dialog between the organization and the certification authority at an early stage. This contact – organization vs. certification authority – must be seen as very important – at least if the organization is planning to seek certification of its ISMS after the implementation.

5.3.7 Summary

The certification auditors in the Swedish pilot certification group viewed these six factors as critical for the successful formation and certification of ISMS (figure 5.2):

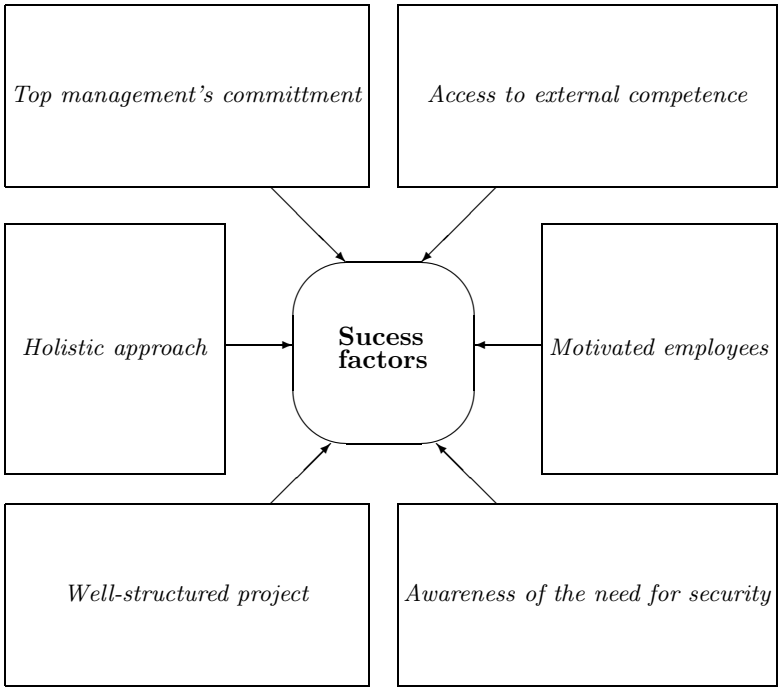


Fig. 5.2: *Success Factors for the formation and certification of information security management systems, from the certification auditors' perspective.*

5.4 Information security consultants' perspective on formation and certification of ISMS

Also for this group, the question was stated as follows (translation from Swedish to English):

> *In your opinion, which are the critical success factors for a successful implementation of an information security management system, ISMS? (Please give reasons for your answer)*

Also here, the answers were analysed using a grounded theory method supported by a computerized data analysis tool (ATLAS/ti).

In total, there were 37 quotations from the consultants on this question. They were first analysed and coded into 23 different categories, using no predetermined codes. This means that the essence of each quote can be represented by its code on this level. Afterwards, these 23 categories were further analysed using the qualitative data analysis tool and we found that they fell into 6 more abstract categories.

Even though all the answers were in Swedish, we decided to code each quotation in English, so that it would be easier to present in this paper. However, the answers were not translated, but they are available in the Swedish report for those interested (see appendices B and C of this thesis).

It should be noted that there is no logic in the data analysis tool to help deciding on the categories of the data. The tool is only used to organize the analysis, and to keep track of and visualize the analysis result.

Here are all the codes used at the first level of analysis (in alfabethical order):

1. ability to put policy into practice
2. accurate analysis of preceding security situation
3. active employee participation
4. active project members
5. appropriate project organization
6. backing from top management
7. balanced policy grounded in reality
8. clear aim from top management
9. customer organization participation
10. documented business processes
11. feasible implementation method

12. identifiable business benefits
13. implementation know-how for project leader
14. insight and knowledge about security
15. integration with existing management systems
16. monetary resources
17. project ability to influence IT development
18. realistic cost estimation
19. realistic time plans
20. regular communication with stakeholders
21. top management awareness
22. top management involvement
23. understanding the need for security

These codes were further analysed and categorized into six more abstract categories. These six categories were:

1. Project management capability
2. Commanding capability
3. Financial capability
4. Analytic capability
5. Communicative capability
6. Executive capability

These capabilities form the foundation for a theoretical framework. Here is a short description of each of these capabilities. Please refer to appendix C for more elaborate discussions of each capability.

5.4.1 Project management capability

A successful implementation project will need to have efficient project management capability. This means that for example active project members, an appropriate project organization and realistic time plans are needed.

5.4.2 Commanding capability

The commanding capability stems from the top management sponsorship of the project. It is this capability that gives the project the authority to decide on issues regarding information security. Without any real decision-making power, it is very hard, if not impossible to do reach the project goals. This capability is given by for example top management awareness and involvement in information security, identifiable business benefits and an understanding for the need of security, and a clear aim and backing from top management.

5.4.3 Financial capability

All information security projects need budgeted resources. A project with this capability is able to estimate costs realistically. It also has access to the resources needed to carry out the project.

5.4.4 Analytic capability

Projects with analytic capability can accurately analyse the preceding security situation, and therefore develop a well-balanced ISMS which is also integrated with existing management systems (e.g. quality and environment management systems – iso900X and iso1400X). In short, this capability is needed to create a balanced policy grounded in reality.

5.4.5 Communicative capability

Many information security efforts stop at the security managers' desk. To avoid this, a communicative capability is needed. This capability is needed to enable regular communication with stakeholders and for active employee participation in the project.

5.4.6 Executive capability

Thinking about security and writing policies is one thing – implementing the ideas, rules, controls, and procedures is another. The executive capability means that the project can do things – that it can make things happen. One of the things that will need to be done is to put the policy into practice and this in turn often requires for example the ability to influence people in the IT department, in IT development and in other parts of the organization. A feasible implementation method and implementation know-how for the project leader are examples of parts that form this capability.

5.4.7 Summary

The information security consultants of the Swedish pilot certification group viewed these six capabilities as critical for the successful formation and certification of ISMS (figure 5.3):

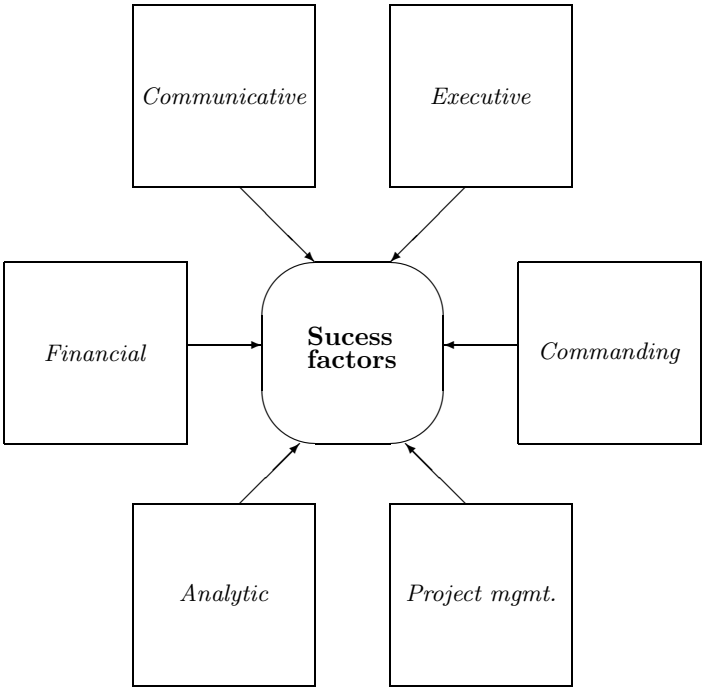
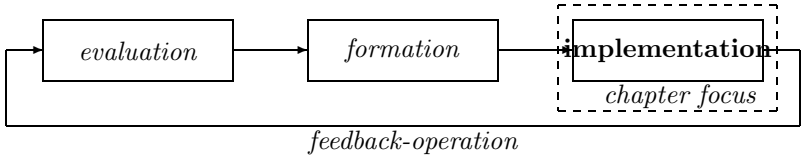


Fig. 5.3: *Success Factors, expressed as project* ***capabilities*** *needed, for the formation and certification of information security management systems, from the information security consultants' perspective.*

5.5 Conclusions

Using an action research inspired strategy and a grounded theory like research method, this study has identified success factors for the formation and certification of information security management systems. Even though we cannot statistically generalize these findings to a broader population, we believe that these results can be useful and valid. Especially for researchers and practitioners working with 7799 and similar management standards.


evaluation
formation
implementation
chapter focus
feedback-operation

6. IMPLEMENTATION STAGE - PAPER C: "VALUE AND ASSESSMENT OF INFOSEC EDUCATION"

Information security education and training needs to be valued and assessed from various perspectives. This study presents two differing viewpoints from which such an evaluation can be perceived – those of the individual and the organisation[1]*. Some sorts of profits are sought after by each of the two, although this is expressed and hence valued differently depending on the perspective taken. From the organisations' point of view, training and education are key activities while implementing information security management systems. In that respect, this paper illuminates some critical issues related to the implementation stage, in which the effectiveness of information security education and training can be viewed as a key performance indicator. In particular, the paper examines; the need, current techniques, and practical problems, related to measuring. The main purpose is to demonstrate the limitations of, and problems related to, current techniques employed when assessing the potential economic impact of information security training programmes*

6.1 Introduction

The Internet evangelium is rapidly embraced everywhere – log onto "The Net" and meet new friends, order that vegetarian pizza, place a phone-call, visit the Museum of Ancient Art, groove to the latest hit, watch the news, make business the modern way - go global! Undeniably, the potential benefits are immense. However, most of us forgot that all coins usually have two sides: "You can pay me now or you can pay me later", as William Murray (1995) phrases it. In the haste to get on-line, organisations and individuals alike have sometimes ignored information security risks. Hence, today the need for information security education and training is more evident than ever.

– The times when only a few experts needed education and training in information security are gone forever. Today, journalists, politicians, managers, parents,

[1] This chapter is based on a previously published research paper (Yngström and Björck 1998). section 6.1 of this paper is co-authored with Yngström, while section 6.2 is entirely written by Yngström, but presented here for purposes of completeness. All other parts of the paper are authored by Björck.

pupils, teachers and other individuals require this type of knowledge.

– The times when the whole body of IT knowledge could fit into the finite domain of computer science are gone forever. Today, ethical, social, legal and economic implications of IT use must be considered - so also within the realm of information security.

– The times when information security could be taught solely in a linear fashion focusing mainly on aspects of confidentiality are gone forever. Today, the information security agenda has changed - aspects such as trustworthiness of information are seen as more important. Further, the new broadened curriculum demand new pedagogical tools – ideally interdisciplinary and holistic approaches.

As the conditions for information security education and training changes, the need for thorough evaluations and assessments are on the rise. This study presents the need for information security education and training, the need for assessing (or measuring the effects of) such efforts, and some examples of methods and problems pertaining to assessment. These three aspects tend to look very different from the viewpoint of the organisation compared to that of the individual. This paper tries to capture these differences by presenting one section about information security education and training from the point of view of the individual and one section from the viewpoint of the organisation. The purpose is to demonstrate the limitations of, and problems related to, current techniques employed when assessing the potential economic impact of information security training programmes.

6.2 The individual's perspective

6.2.1 The value of and need for information security education and training

It is hardly possible to develop adequately secure IT systems and information management procedures unless high quality education and training in information security is available to individuals – system developers as well as users and others. The vast majority of all information security education and training efforts have been aimed at computer specialists, while other groups such as professional users from other disciplines as well as regular and casual users and usees have been overlooked. As a result, these computer specialists have provided the world with advanced information security models, methods architectures and tools. Unfortunately, many of these have proved to be insufficient or too complex to use. Consequently, the need to educate and train also other groups of individuals in the art of information security has recently been noticed. Selected arguments from these information security scholars reiterates and reinforces this belief:

Highland (1992) suggests that the failure to develop meaningful computer security practices have to be shared by three communities: The academic community which has been lax in acceptance of computer security, the business community which was unable to specify its needs, and the military establishments which has designed models unsuitable for the real world.

Cohen (1995) suggests historical reasons; the important constituents of the information protection domain were separated into the sub-fields of cryptography, computer security, fault tolerant computing and software safety. Computer security covers leakage, fault tolerant computing covers accidental events, and special purpose systems cover selectively otherwise uncovered areas. Specifically, taken together these sub-fields do not cover the full range of information protection and security (*e.g.* disruption of services not attended to).

Parker (1995) argues that defining the elements of information security, as the preservation of confidentiality, integrity and availability is a dangerously oversimplified definition that has to be extended. This definition is not sufficiently comprehensive to protect information appropriately in all of its security aspects.

Fåk (1995) argues we are lacking awareness; we have a market with too many customers knowing neither what they want nor what they can get. There is no lack of basic tools but a severe lack of good implementations. Moreover, experts and practitioners are not interested in each other's questions, thus they do not communicate.

These statements should be taken seriously - lack of meaningful computer security practices, separation of the information protection domain into sub-areas, incomplete definitions, and inadequate awareness. They have in common that they mark the need for information security education and training, not only

for computer specialists, but also for individuals in other positions. Moreover, these sceptical statements about information security imply that evaluations of today's education programmes and training efforts might be deficient.

6.2.2 The need for measuring

From the perspective of the individual/learner, there are several reasons why assessment of education and training efforts ought to be undertaken, *e.g.*:

- Existing education and training on various levels do not yet cover the full range of needs, even though there is a positive trend in numbers of courses, offered by universities and other organisations. Through making explicit areas for improvement, an assessment effort may play a significant role in ensuring that future courses and academic programmes advance to be more all encompassing.
- Depending on the their present stage in life, individuals might strive to get a job, to obtain a better position, to gain higher self esteem, or to perform tasks at work more efficiently and effectively. In whatever situation the individual is in s/he is looking for knowledge that can make their life (or others) a little bit better – individuals want their knowledge to help them earn profits - not necessarily purely financial. Assessment of courses and programmes in information security can assure this in two ways: Firstly, assessment support advancing and sustaining the quality of the knowledge that is delivered to the individual. Secondly, given that the assessment leads to a high quality course or programme, it will attract individuals eager to learn information security, which will further increase the quality.

The necessity to evaluate information security education and training is now apparent, although choosing the scope and the method of evaluation is not always as simple. National Institute of Standards and Technology (1998), in their special publication on 'Information Technology Security Training Requirements' suggests an assessment should cover the learner's subjective satisfaction, the learning effectiveness, the teaching effectiveness and the program effectiveness. For each of these four levels they describe three types of programmes - basics/literacy, training and education. This scheme covers aspects pertaining to the individual, the organisation and, to some extent also societal aspects. In the following section, we will present evaluations focusing the aspects of the individual and the pedagogical methodology. Even though the outcome of such an assessment depends on the students and teachers, organisations and societies later estimate the value of the education or training effort indirectly – on the job market.

6.2.3 Techniques for measuring – an example

General. Yngström developed a similar approach to evaluation as that suggested and described by NIST (1998), in Yngström (1988, 1989, 1991, 1993, 1996). This approach was used for evaluating an interdisciplinary and holistically oriented academic IT security programme. The evaluation also included

assessment of a specific pedagogical methodology chosen to fit the interdisciplinary and holistic approach.

Background – evaluation setting. The educational programmes involved were initially two one year programmes, one on undergraduate level (Bachelor) and one on graduate level (Master) at the Department of Computer and Systems Sciences (at Stockholm University / Royal Institute of Technology in Stockholm, Sweden), in what became labelled as the Security Informatics Programmes. These programmes were later split into smaller units, which also were involved in the evaluations. Also an evaluation of a single IT security course including the pedagogical methodology, offered in a non-European university environment was included. The development of programmes and their courses began out of need and curiosity. The Swedish Vulnerability Board had recommended all educational institutions, including universities, to initiate courses in (then) EDP security, and practical circumstances made us hypotheses that a specific pedagogical methodology using system theories would be a useful vehicle to understand interactions between technical and non-technical components needed for secure IT environments. The courses were originally developed in interaction between members of the Vulnerability Board, industry and academia (Yngström 1983). As an educator it is fundamental to see what happens. But how should such courses be evaluated, their main goal being to lessen vulnerability in trade, industry, government, and societies? It was quite clear from the beginning that the primary groups to be educated would be managers responsible for the enforcement and measures of safety and security in computer systems at different levels of society and organisations. Therefore the initial target group for education was specified as managers, or managers-to-be, of security in organisations that use computers, and the intent was to increase the professionalism within these groups by providing them with a specialised undergraduate degree that would also qualify for entering graduate studies. The goals of the first programme on undergraduate level were stated as:

> Of such an extension and be placed at such a level that width and depth, theoretically as well as practically, will bring the student ability to participate independently in the processes of planning, designing, implementing, evaluating systems and -functions which will lead to that the demands of reality for system survival can be realised. In this context the concept system does not only imply technical ones (like computer-, communications-) or administrative ones (information-, surveillance-) but the total reality including the artefacts needed to create stable and robust structures on different levels of society. (Yngström 1983, 297).

Early evaluations to refine the programme. The first evaluations were regular pedagogical ones, concerning aims and scopes, course structures, contents, levels, modes of presentation, literature, examinations, overall structure, acquired attitudes, conducts and abilities and involvement from industry. These were conducted annually from the beginning and used mainly to trim the programme. In these evaluations it also became interesting *vis-à-vis* the chosen

target group to see how active and what specific activities outside the class room participants were involved in. This made us include various statistics in the evaluations such as previous experiences from traditional security or IT security, previous academic studies in various disciplines, memberships of professional associations concerned with IT security or other relevant areas, *etc.*

Evaluation of the use of system theory as a means of teaching. Not until the courses and the programme had been found good enough, that is, when the students were happy with most of the aspects and could use the knowledge at work, was it time to investigate whether the original methodological idea of using system theories was of any use to them. This was in 1991 formulated into ten practical statements and presented to all students ever in the programme five years after its start in 1986. The statements dealt with different aspects of the practical use of system theories: their contribution to the students' awareness of appropriate problems and their ability to deal with these, their contribution to students' abilities to work efficiently and effectively and their contribution to the ability of continuous learning.

Design of the evaluation and evaluation questionnaires. The ten practical statements mentioned above were classified into three categories, and answers were marked on a scale 1-5 ('1' meaning agreeing fully and '5' not agreeing at all). It was also possible to answer 'question not relevant to me'. In order to know something about the market's opinion of these former students' abilities and knowledge in the area, questionnaires also asked for evidence of promotions and positions before and after the programme. By this time, about one third of the former students were professionals in the traditional security and IT security industries; a small group of which promotions and activities it was possible to keep track of even manually at this time. In parallel was kept also statistics of students' backgrounds, memberships, etc. This group of former students formed the Swedish Association for Information Security (SAIS) to promote further academic education in the area. A top priority was to increase the amount of courses, and this became the embryo to the Master programme in Security Informatics, which separate courses initially were given within the PhD programme of the same academic department. The evaluation design of the, for the first time ran, Master programme in 1993/94 show similarities with the very first evaluations of the Bachelor programme in 1986/87; the aim being to find out whether the programme met the needs of the students and the market, and to trim it into a scientifically and pedagogically esteemed programme. The demands for knowledge in the area changed and widened during the time the two programmes have existed; regular bachelor and master students in Computer and Systems Sciences demanded to take some Security Informatics courses during their last academic year. This made the Department divide the Security Informatics programme into four units, of which three are units of two courses, each which may be chosen by regular students. This change became evident in the evaluations of 1992-94, where the usefulness of the pedagogical approach was investigated in the same way as in 1991, but this time directly after the students had finished the first unit. Many of these students had not yet started their careers and could only react to statements concerning the approach's contribution

to their general abilities to handle IT security. The general statistics were also collected for further comparisons. Since the specific methodology as such is strongly influenced by the North European movements of participatory design and Soft Systems Methodology, we were specifically interested to know how the approach would be rated in a non-European culture. Therefore the 1992-94 evaluations include reactions to the statements also from one Australian group of honour students. This group was however fairly small.

Evaluation results. The results from the 1991 study was summarised as follows:

> When it came to the assessment of whether the methodology chosen positively contributing to this group's ability of problem awareness, work efficiency and effectiveness and continuous learning, 92% agreed with this. In agreement to at least 50 % were the 50 professionals within the security area. The approach contributed the most to a person's ability to delimit and specify her own problems and work tasks, but also to her ability to specify for others, such as colleagues. Relatively high scores were attributed to specifying criteria for security products, to work efficiency and learning about new products, methods and facts. The contributions to the ability of working with new products and controlling the work of consultants scored the lowest. However, with a mean score of 45.9 persons being positive to all the ten statements, the chosen methodology is perceived to have contributed to these people's ability to cope with traditional security and IT security.

The result of the 1992-94 studies were summarised as follows:

> The low frequency of practical experiences in security and IT security made it impossible for the students to answer half of the statements, and also to compare reactions to all ten of them. Still, answers not referring to work experiences show high appreciation; in all the mean positive reaction to these five is 46.8 out of 60. For statements requiring work experience the positive mean was 7.6 out of 11. Based on the means, 78% were positive to the non working related statements and 69% to the working related ones.

A comparison between answers given by Australian and Swedish students was interesting but results were non-conclusive. Swedish answers by all - practitioners and students - were higher rated than the Australian answers and there were no particular similarities in the individual ordering of the answers between the Swedish and the Australian students. When comparing the answers between Swedish and Australian practitioners, they varied more positively in different statements.

Comparison and analysis of the different evaluation results. A special analysis of the results of the 1991 and 1992-94 studies was made, where answers

	1987	1991	1992-1994	1993-1994
Population (N)	72	155	120	26
Answers (n)	72	71	60	11
Professionals in (IT) security	47%	70%	18%	91%
Pros. in other positions	60%	10%	38%	9%
Mean age	33	34	30	32
Women ratio	11%	13%	32%	9%
Academic sucess ratio	81%	46%	83%	46%
Educational background: CS	47%	70%	85%	100%
Educ. bgr.: BA, Econ. or Law	40%	51%	48%	100%
Satisfactn. pedagogical method	n/a	92%	69%pro 78%all	89%

Fig. 6.1: *Some general characteristics of the students*

were weighted in order to be able to compare them. This analysis showed that that the approach helps in forming personal learning models and acquiring good insights; and best for Swedish university students, second best for Swedish professionals, and thirdly for Australian university students. However, we do not find it reasonable based on such small groups to predict where the approach works best. The differences in duration of presentation, possibilities to try in practise and other factors were too large, in addition to the small size of the Australian group. Judging the figures in total may at least be used as an indication, pointing to the positive reactions favour in total used pedagogical methodology. It may be reasonable to interpret the result as the Systemic-Holistic Approach and the Systemic Module facilitate individuals to assess and understand problems, increase work efficiency (doing things right) and effectiveness (doing the right things) and foster continuous learning within the field of security and IT security - provided the student has some own experience to refer to. When students do not have their own work experience, Systemic-Holistic Approach and the SM still facilitate assessment and understanding of problems, increase of effectiveness (doing the right things) and fostering of continuous learning - but in order also to increase efficiency (doing things right) practise is needed. Assessment of the Master Programme included a question of where and if the approach had been useful. Eight of the eleven students noted "in all courses", and the other three offered varying, but positive answers. In addition all students rated the programme as a whole to have fulfilled their different educational goals positively, giving a mean of 89% of the successful students. We would regard that as qualitatively very good answers; the organisation and presentation of the content had been more than satisfying to all participants even despite different educational goals. Also the Master programme has shown to be efficient within the market for its successful participants; participants are satisfied with the programme and employers are happy to hire and promote them.

Figure 6.1 (table) was constructed in order to describe and discuss some other similarities and differences between the groups being evaluated in 1987, 1991, 1992-94 and 1993/94. Separate figures were taken from (Yngström 1996, 176) or compiled based on it. It is not the separate figures that are interesting, but they may reveal emerging trends:

Groups 1991 and 1993/94 are the most alike in professional attitudes and am-

bitions; they have a high percentage of traditional and IT security professionals with a low percentage of other professionals. At the same time the academic success rate in total of all starting students is below 50% for both groups. They also have in total the highest figures for the value of the Systemic-Holistic Approach and the Systemic Module. Other figures of interest to note are: fewer women seem to be engaged in groups with higher professional attitudes and ambitions, the age of professionals seems to be lowering, and the group is totally well educated in more than one academic discipline.

The 1992-94 group was already earlier noted as a typical university students group. It includes fewer professionals in traditional security and IT security. Members are younger, and also more women participate. The academic success rate is the highest of all groups. In total their appreciation of the SM and the S-HA is somewhat lower than the professional groups.

The 1987 group could be labelled as 'old boys' - not because of its low participation of women, but because it contained an enthusiastic first lot of varied practitioners with varied backgrounds and very strong wills to build good security foundations. Their academic success rate was as high as the students group although their theoretical backgrounds initially were lower than all other groups. Members of the 1987 group later on have moved into the 1991 group. Possibly the high percentage of professionals from other areas in 1987 have become professionals in traditional and IT security in 1991. Satisfaction rates with the Systemic-Holistic Approach and the Systemic Module are for 1991: 92%, 1992-94: 69% for statements answered only by professionals and 78% for statements answered by all, and 1993/94: 89%. Despite the fact that the groups as compared to each other they are quite different; 1987 being 'old boys', 1991 being IT security professionals, 1992-94 being regular university students, 1993 being a non-Swedish university group, and 1993/94 being a highly professional group, they all were in favour of the pedagogical methodology with satisfaction rates about 70-90%. It seems therefore reasonable to state that the methodology was useful to students of IT security. In addition, the strong involvement of professionals in the programmes showed that former students make good careers with increased salaries, high esteem and promotions, both as managers and specialists.

Scientific limitations of the evaluation approach. The presented example of evaluations is not claimed to be generalisable in detail, which was not the intentions at the time. However, the approach to evaluate the programmes on different levels as described by NIST (1998) was followed; student satisfaction with the courses in various aspects were evaluated, the learning effectiveness and efficiency were evaluated for performances within the education as well as performances and outcomes at the workplaces, and the long run effectiveness of the programmes were evaluated career-wise for former course participants.

These evaluations and comparisons were all carried out without using control groups, since at the time there were no comparable courses and programmes. Today it would be possible to use the same kind of evaluation tools: questionnaires, interviews, and inspections of examination and seminar-work results, for different courses and programmes. This would certainly, to students and educators, be of value for instance choice of institution or course revisions and devel-

opments. However, measuring the value in some sense of information security training and education, in the opinion of these authors, needs some standard or index to be measured towards. In academic environments such standards exist, although they may vary from country to country, from university to university or from one professional group to another. In the information security area for professionals, such standards also exist in various types - typically named certificates, - initiated as a qualitative metric. We believe all such certificates, academic as well as professionals will be of use, but we also acknowledge that the area of information security is a moving target, hence a certificate of some kind will not suffice as a general measurement, but has to be supplemented with something more; maybe some form of index which will consider at least the age and content of the separate certificates. But not only is the area of information security a moving target, it is also partly a context-oriented issue - it is global in the sense of networking possibilities and it is local in the sense of existing social values and particular application areas. Such factors should probably also be weighted into an index.

This concludes the presentation of; the need, techniques, and practical problems, related to measuring the effects of information security education and training from the perspective of the individual. Now, let us have a look at the same issues but from the organisation's perspective.

6.3 The organisation's perspective

6.3.1 The value of and need for information security education and training

From the viewpoint of an organisation, information security not only promises to assist safeguarding information assets at a given cost but, more importantly, it can provide the organisation with a competitive advantage through lower costs and new business opportunities (*e.g.* Wood 1991, Parker 1997). Thus, organisations – from corporations through hospitals to government agencies – are increasingly becoming aware of the need to safeguard their information. At the organisational level, this is usually accomplished utilising technical as well as procedural measures – *all of which depend upon human behaviour and skills to perform*, for example:

- *Technical measures*: Installing, configuring and maintaining a secure Internet firewall will only succeed if the persons involved understand the elementary concepts of TCP/IP network traffic, have a good grasp of what inbound and outbound communications are needed, and are familiar with the interfaces used to accomplish the tasks at hand.
- *Procedural measures*: Handling information in the way described by an organisation's information classification scheme might require the understanding of how, for example, one uses the backup system on the office workstation and how one can positively verify the sender of a digitally signed document.

This fact – that the human factor is one of the most significant determinants of the overall success of information security efforts in an organisation has been pointed out in several recent empirical studies on information security in organisations. The following citations confirm this actuality:

- Employees' information security awareness is perceived as the most important means to overcome the security problems (Björck 1998).
- According to RRV it is important that awareness of computer related crime and abuse is raised within the management structure of organisations. It should be a primary priority of management to work to reduce the risk and threat from the different kinds of computer crimes. These problems cannot simply be solved by buying-in more technology. (Riksrevisionsverket 1997).
- "This study's main conclusion is that the respondents consider the main threat against the organisations' EDP stored information to be employees' unintentional and erroneous change and deletion" (Johansson and Kager 1995).

By now it is evident that most organisations seems to need information security education and training, and that they are likely to benefit from information security education and training efforts. However, organisations do not usually dedicate resources for projects with no measurable impact.

6.3.2 The need for measuring

Managers make organisational decisions in a way similar to the way most individuals make personal decisions – with bounded rationality. In an ideal world, that means they will try to reach the optimal decision, from the viewpoint of the organisation's purpose, given the information available at the time of the decision. Decisions regarding investments in information security education and training are also likely to follow a similar decision process. Strategic decisions (those that have a considerable impact on the organisation) are usually approached in a more structured manner than less consequential operational or tactical decisions. Regardless of the importance of a given decision, some kind of cost-benefit analysis is always carried out before a decision is arrived at – either implicitly or explicitly. Given that organisations have a finite amount of resources to employ in the pursuit of its mission, investments in information security education and training must compete against other possible investments. The actual decision process probably does not follow the logical path described here, since many decisions are arrived at for other reasons than purely rational ones (*e.g. political, power, etc.*). Nevertheless, these rational decision models are often brought forward before or after a decision to rationalise[2] a decision to be made or a decision already made.

6.3.3 Techniques for measuring – an example

A simplified example serves as an illustration on how organisations generally rationalize decisions regarding investments:

A manufacturer of studio quality microphones has 100.000 Euro reserved for investments in a given period of time. There are many different areas in the organisation that would benefit from new investments, such as a new microphone-assembly machine. In addition, there is a need for a comprehensive information security education and training programme. However, the monetary resources will not be sufficient for all desired investments, so a choice has to be made. Given the dissimilar nature of these investments, the impact of each will first have to be translated into monetary terms, so that a comparison is possible. Moreover, since these investments (if realised) will have an economic impact on the organisation at different moments in the future, the value of money must be converted into a common point in time – for example the day of the decision. Let us have a look at the two competing options.

Alternative I - investing in the machine. The new machine would cost exactly 100 K Euro and result in yearly operating costs of 10 K Euro for each of the subsequent five years. After this period, the machine would need to be replaced, but it could be sold for an estimated 5 K Euro (figure 6.2).

The machine would produce microphones using the components put into the four containers on the side of it. Based on sales statistics from previous years, the microphones produced by this machine will generate 60 K Euro in sales

[2] 'Rationalise', as used here, refers to the process of justifying ones actions with plausible reasons.

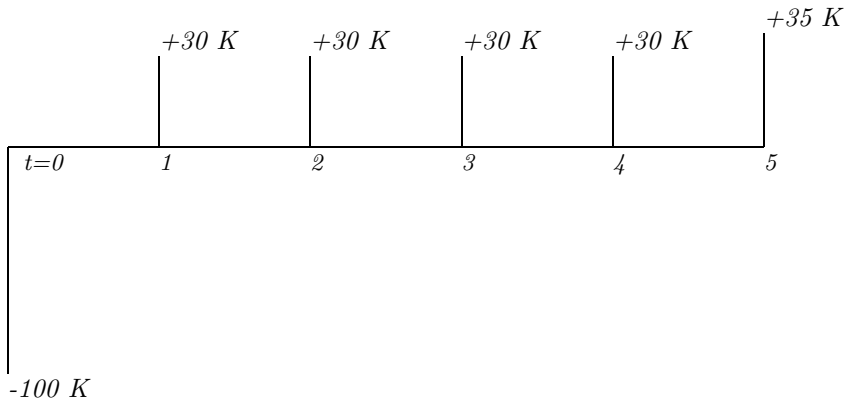


Fig. 6.2: *Expected payment flows resulting from investment in the microphone-manufacturing machine*

each of the five years, of which roughly 20 K Euro are costs for components, marketing, Etc. Thus, the net payments generated by this investment during these five years following the initial investment will be 30 K Euro (60 K Euro for sales payments, less the 20 K Euro for components and various costs, less the 10 K Euro for the machine's operating costs). If the machine is sold as predicted, the final year of operation will result in an additional 5 K Euro of net payments. These flows of payments are illustrated in figure 6.2. The value of this investment alternative can be calculated as the sum of all transactions relevant to the investment – in this case:

(-100) + (+30) + (+30) + (+30) + (+30) + (+30) + (+35) = 85 K Euro

However, since the payment flows take place at different moments in time, they need to be converted into their present value, taking into account the cost of capital (interest rate). This is because the resources could have been used for some other investment which would have produced a calculated payoff or return on investment (R.O.I.). Let us assume that if the organisation would not have used the money for this investment, it could have bought some stocks instead and these would yield 15% R.O.I. per year. Therefore, this is the estimated capital cost if investing in the machine. Consequently, the present value PV, of the net payments of *for example the third year* can now be calculated as (figure 6.3):

$$PV = \frac{C}{(1+r)^t} \Longrightarrow PV = \frac{30}{(1+0.15)^3} \approx 20KEuro$$

Where C=capital, r=interest rate, and t=time/year

Fig. 6.3: *The present value (PV) of investing in this alternative*

All of the net payments (including the initial cost of the machine) resulting from this investment alternative will have to be converted into their present value if we want to be able to compare this investment with the investment in information security education and training. With this conversion, we will end up with the investments net present value NPV, as illustrated in figure 6.5.

$$NPV = C_0 + \frac{C_1}{(1+r)} + \frac{C_2}{(1+r)^2} + ... + \frac{C_n}{(1+r)^n} \Longrightarrow NPV = C_0 + \sum_{k=1}^{n} \frac{C_k}{(1+r)^k}$$

NPV=-100+(30/1.15)+(30/1.32)+(30/1.52)+(30/1.75)+(35/2.01)=103 K Euro

Where NPV=net present value, C0=initial payment, Ck= other net payments, r=interest rate, and n=number of payment periods(years)

Fig. 6.4: *The net present value (NPV) of investing in this alternative*

As we can see in the calculations above, the net present value of the investment in the microphone-manufacturing machine is 103 K Euro. This can be interpreted as "If we take into account that the alternative investment would have given us 15% interest rate, we would gain 103 K Euro if we invested in the machine".

Now it is time to compare this investment with that of investing our resources in the information security education and training programme. Converting the information security education and training investment into its NPV makes the two investments comparable – the one with the highest NPV is the one the resources should go into if we are to make the optimal investment decision.

Alternative II - investing in information security education and training. The ISET programme would consist of an information security awareness project aimed at different parts of the organisation, as well as some specialised information security courses for the individual's co-ordinating the information security activities in each department. The whole ISET programme would mean an initial investment (for course material, speakers, teachers, and external courses, *etc.*) of 50 K Euro, and additional yearly costs of 10 K Euro for each of the subsequent five years. After these five years, the program will be evaluated. Naturally, the information security education and training investment does not have any residual value that can be converted into funds the final year, since it cannot be sold or transferred to another organisation with ease. So far, we have identified the following flow of payments for this investment alternative (Figure 6.5).

Investment calculations usually only take into account the direct payment flows that result from the analysed investment. Therefore the investment in information security education and training does not look very good in comparison with the investment in alternative I. In fact, as observable in the calculation below, investment in the information security education and training programme will result in a negative NPV unless other payment flows than the calculated yearly costs can be identified:

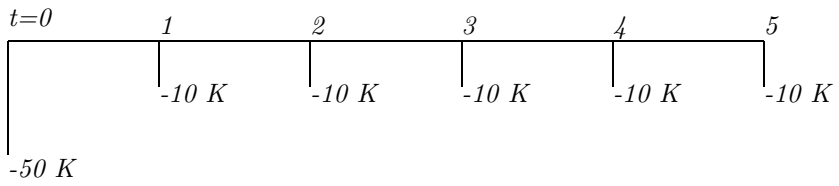


Fig. 6.5: *Expected payment flows resulting from investment in the information security education and training programme*

NPV=-50+(-10/1.15)+(-10/1.32)+(-10/1.52)+(-10/1.75)+(-10/2.01)=-83 KEuro

The investment in information security education and training is likely to have a long-term economic impact on the organisation, in terms of cost reduction due to less severe and fewer information security breaches. Also, the information security education and training programme might possibly enable new business transactions to take place, as pointed out in previous sections of this paper. If organisations, using this rational financial model of comparing investments, are to choose the investment in an information security education and training programme instead of other investments, *indirect payments flows resulting from this decision must be taken into account*. If these indirect payments and economic effects can not be identified, it will not be possible to rationalise the investment in information security education and training.

From the example, it is evident that organisations will have to try to measure *the impact of* information security education and training if it is to be a viable investment at all. Unless organisations are given the tools to identify the value of their education and training programme, they will not be able to justify such an investment. As a result, resources will be invested in other areas with a measurable payoff.

What can we learn from this illustrative example? This section has made explicit how organisations, according to financial investment models, generally rationalise their decisions regarding where to invest its limited resources. It has thereby clarified why organisations need to measure the broader *impact* of information security education and training. Is it evident by now that this purely financial and cash-flow perspective may severely limit the organisation's ability to make accurate and balanced investment decisions with regards to information security education and training. This leads us over to a discussion on possible information security education and training metrics and the problems associated with measuring.

6.3.4 Methods and problems of measuring

While measuring the impact of information security education and training, one is actually trying to measure the resulting change in human behaviour and its

impact on the organisation's ability to reach its goal. There are several problems associated with measuring the impact if an organisational information security education and training effort, such as:

Discrepancy between what people say and what they do. The mere fact that employees, through an information security education and training programme, arrive at a measurable raised awareness of the information security regulations does not signify that they actually follow these rules or values – at least not all of them. Further, when trying to measure the impact of information security education and training, there is a possibility that some employees *do not* want to state the truth about their own level of awareness. They might be anxious concerning what the employer's reaction would be if they admitted that they did not know of the rules they were supposed to adhere to. Therefore, from an organisational perspective, the focus should not be on what an employee knows about information security, but rather what she does with this knowledge.

Interpreting the numbers. Common sense tells us that it will be hard, or maybe even impossible, to put a number on "soft" issues, such as information security awareness (*e.g.* Dhillon 1995). However, exact numbers are very seldom needed for an informed decision. Rather, some kind of grading, judgement or comparison is often needed. Another problem is that once numbers are produced, it might be hard to interpret them. What does it mean, for example, if the level of information security awareness is around 70%? Is this good, or is it bad? The exact answer is; we don't know. In order to interpret numbers like these, the context have to be clear – is it a bank, or is it a fast food chain? How dependent are they on their information? Quantification of "soft" issues is more useful if it can be compared with something else as a reference. For example, the level of information security awareness as measured in one financial institution might be seen in the light of the measured average level of information security awareness in all other financial institutions in that region (given that the method for measuring was the same).

What should be measured. Information security education and training is an extensive concept in itself - it embraces many facets of information security. In our view, information security awareness is manifested in the behaviour of the humans enlightened with it. This means that the action created by bright humans causes effects measurable only outside the finite domain of human knowledge or behaviour - in the technical and procedural elements of the organisations information system. Since some, or presumably large proportions, of these effects are directly caused by the intellectual capital labelled information security awareness, one can conceive that the estimation of these must be conducted within the formal and technical domains.

Assuming that rationalisation of investment decisions approximately follow the decision method outlined in the example in the previous section, organisations cannot be satisfied with measuring or predicting an information security education and training programmes impact on employees knowledge only. No, this raised awareness must result in a corresponding change in human behaviour. In addition, this change must result in either lowered costs or increased revenue.

6.4 Conclusions

This study has demonstrated how differing the viewpoints of the organisation and the individual are when it comes to information security education and training.

Individuals - we do not only mean computer specialists - need for information security education and training to be able to minimise their security risks that they are, and will be, exposed to today, and in the approaching information society. In addition, they want this kind of training to make them appear more valuable for the organisations. Organisations' needs are often more directly connected with their financial mission or goal. This often means that they look for information security education and training to lower costs arising from information security breaches or for enabling new business opportunities.

Organisations need to measure the effects of information security education and training because of their decision process for investments. Looking at these education and training efforts as any other investment, they demand a reasonable "return on investment" to rationalise the decision. If they are not provided with methods to measure the effects of, for example, a training programme, they will not be able to identify changing cost or income structures resulting from this effort. This leads to that the investment in education and training will look less favourable than it really is.

From the viewpoint of individuals, assessment of these education and training efforts should ideally focus on the knowledge content. Organisations, although indirectly attracted by the knowledge, are often more interested in the behavioural changes a given course or programme can result in. This is, as we have seen, because the knowledge has to result in some change in behaviour if it is to be valuable not only for the individual, but also for the organisation. Individuals are looking for profit and so are the organisations, but their respective approaches and focuses in regard to value and assessment of education and training are sometimes incompatible.

7. REFERENCES

Bell, D.E., and L.J. LaPadula. 1974. *Secure Computer Systems: Mathematical foundations and model.* Bedford, Mass: MITRE Corporation. M74-244.

Björck, F. 1996. *The Economics of Information Systems Security.* London: London School of Economics, Department of Information Systems. Unpublished report.

_____. 1997. *Information Security Survey Sverige 1997.* Stockholm: Ernst & Young AB. (Based on 541 survey responses from Swedish IT- and Information security managers).

_____. 1998. *Information Security Survey Sverige 1998.* Stockholm: Ernst & Young AB. (Based on 428 survey responses from Swedish IT- and Information security managers).

_____. 2000. Auditing Information Security Management Systems - Towards a Practical Method. In *IFIP/SEC2000: Information Security – Information Security for Global Information Infrastructures, Proceedings of the IFIP TC11 16th annual working conference on information* held in Beijing during the World Computer Congress, August 21-25 2000, edited by Qing S. and J. Eloff. Beijing: International Academic Publishers.

_____. 2001. Implementing Information Security Management Systems - An Empirical Study of Critical Success Factors. In *Advances in Information Security Management & Small Systems Security, Proceedings of the eighth annual working conference of WG 11.1 and 11.2 of technical committee 11 part of International federation for information processing, held in Las Vegas 27-28 September 2001 (conference was postponed due to the September 11 terrorist attacks in the USA)*, edited by Eloff, J.H.P., L. Labuschagne, R. von Solms and G. Dhillon, Boston: Kluwer Academic Publishers.

Björck, F and L. Yngström. 2001. IFIP World Computer Congress / SEC 2000 Revisited. In *WISE 2, Proceedings of the IFIP TC11 WG 11.8 Second World Conference on Information Security Education, held in Perth July 12-14.* edited by Armstrong, H. and L. Yngström, 209-223. Perth, Australia: International Federation for Information Processing.

Brewer, D. 2000. *Web site http://www.gammassl.co.uk accessed 2000-02-10*, London: Gamma Secure Systems Limited.

BSI (British Standards Institute). 1999. *Information Security Management – Part 2: Specification for Information Security Management Systems (British standard BS 7799-2)*, London: British Standards Publishing Limited.

_____. 2000. *Information technology - Code of practice for information security management. (British standard ISO/IEC 17799, BS 7799-1).* London: British Standards Publishing Limited.

BSI (Bundesamt für Sicherheit in der Informationstechnik). 2001. *IT Baseline Protection Manual - Standard security safeguards.* Available online from http://www.bsi.bund.de/gshb/english/menue.htm. Accessed 2001-10.24. Bonn: Bundesamt für Sicherheit in der Informationstechnik).

Burrell, G. and G. Morgan. 1979. *Sociological Paradigms and Organisational Analysis.* London: Heinemann.

Checkland, P. 1981. *Systems Thinking, Systems Practice.* Chichester: John Wiley & Sons

Cohen, F.B. 1995. Viruses, Corruption, Denial, Disruption and Information Assurance. In *Information Security - the Next Decade, Proceedings of the IFIP TC11 11th annual working conference on information security*, edited by Yngström, L. Amsterdam: Kluwer Academic Publishers.

Computer Economics. 2001. *Computer Economics Virus Impact Update.* Available on-line from http://www.computereconomics.com. Accessed 2001-09-15. San Diego: Computer Economics.

Cresson Wood, C. 1991. Using information Security to Achieve Competitive Advantage. *Journal of Computers & Security* 10: 399-404.

CSI (Computer Security Institute). 2001. *Computer Crime and Security Survey.* Available on-line from http://www.gocsi.com. Accessed 2001-09-15. San Fransisco: Computer Security Institute. (Based on survey responses from 538 computer security practitioners in U.S. organisations).

Cyert, R.M. and J.G. March. 1963. *A Behavioural Theory of the Firm.* Englewood-Cliffs: Prentice Hall.

Deming, W. E. 1986. *Out of the Crisis.* Cambridge, Mass.: Massachusetts Institute of Technology Center for Advanced Engineering.

Denscombe, M. 1998. *The Good Research Guide*. Buckingham: Open University Press.

Dhillon, G. 1995. *Interpreting the management of information systems security*, Ph.D. diss. London: The London School of Economics and Political Science, Department of Information Systems.

Eloff, M.M. and S.H. von Solms. 1998. Measuring the information security level in an organisation. In *Information security – small systems security & information security management: Proceedings of the sixth working conference of WG 11.1 and 11.2 of technical committee 11 part of International federation for information processing, held in Budapest 2 September 1998*, edited by Eloff, J.H.P. and R. von Solms, 16-30. Laxenburg, Austria: International Federation for Information Processing.

_____. 2000a: Information Security: Process Evaluation and Product Evaluation. In *Information Security for Global Information Infrastructures: Proceedings of the IFIP TC11 16th annual working conference on information security at the World Computer Congress held in Beijing, 21-25 August 2000*, edited by Qing, S., and J.H.P. Eloff. Amsterdam: Kluwer Academic Publishers.

_____. 2000b. Information Security Management: An Approach to Combine Process Certification And Product Evaluation. *Journal of Computers and Security* 19, no. 8: 698-709.

Ernst & Young. 2001. *Information Security Survey*. Available on-line from http://www.ey.com. Accessed 2001-09-15. Cleveland: Ernst & Young. (Based on 237 responses from structured interviews, face to face and via telephone, with CIOs and business executives in Europe).

_____. 1999. *2nd Annual Global Information Security Survey*, Cleveland: Ernst & Young LLP.

Falk, Thomas and Nils-Göran Olve. 1996. *IT som strategisk resurs*. Malmö: Liber.

Fillery-James, H. 1999. *A Soft Approach To Management of Information Security*, Ph.D. diss. Perth: Curtin University of Technology.

Fåk, V. 1995. Unused tools are useless or Why is the gap between theory and practice in network security so wide. In *Information Security - the Next Decade, Proceedings of the IFIP TC11 11th annual working conference on information security*, edited by Yngström, L. Amsterdam: Kluwer Academic Publishers.

Glazer, R. 1993. Measuring the value of information: The information-intensive

organization. *IBM Systems Journal* 32, no. 1: 99-110.

Glaser, B.G. 1978. *Advances in the Methodology of Grounded Theory: Theoretical Sensitivity.* Mill Valley, CA.: Sociology Press.

_____. 1992. *Basics of Grounded Theory Analysis.* Mill Valley, CA.: Sociology Press.

_____. 1998. *Doing Grounded Theory: Issues and Discussion.* Mill Valley, CA.: Sociology Press.

Guba, E.G. 1978. *Toward a methodology of naturalistic inquiry in educational evaluation* (Monograph 8). Los Angeles: UCLA Center for the Study of Evaluation.

Guba, E.G. and Y.S. Lincoln. 1989. *Fourth generation evaluation.* Newbury Park, CA: Sage.

Highland, J. 1992. Perspectives in Information Technology Security. In *Proceeding of Education and Society - Information Processing '92.*

Humphreys, E.J., ed. 2001. *Draft BS 7799 Part 2 (version D)*, London: Photocopied.

Humphreys, E.J., R.H. Moses, and A.E. Plate. 1999. *Guide to Risk Assessment and Risk Management*, London: British Standards Institute.

Insight Consulting. 2001. *Insight on CRAMM IV.* Available online from http://www.insight.co.uk/pdf_files/CRAMM%206pp%20NEW.pdf. Accessed 2001-10.24. Walton on Thames: Insight Consulting Limited.

ISACF (Information Systems Audit and Control Foundation). 1996. *Control Objectives for IT and Related Technologies*, Rolling Meadows, IL.: Information Systems Audit and Control Foundation, IT Governance Institute.

_____. 1999. *Control Objectives for Enterprise Governance*, Rolling Meadows, IL.: Information Systems Audit and Control Foundation.

_____. 2000. *Control Objectives for IT and Related Technologies, third edition*, Rolling Meadows, IL.: Information Systems Audit and Control Foundation, IT Governance Institute.

ISO (International Organization for Standards). 2000. *Information technology - Code of practice for information security management. (International standard*

ISO/IEC 17799:2000). Geneva: International Organization for Standards.

Johansson, H. and M. Kager. 1995. *Perceived Threats Against Information in ADP-Systems. A Study of Swedish DP-Managers Perception*, MSc. thesis. Stockholm: Stockholm School of Economics, Department of Information Management.

Knight, F.H. 1921. *Risk, Uncertainty, and Profit.* Boston: Houghton Mifflin Company.

Kowalski, S. 1994. *IT insecurity : A multi-disciplinary inquiry*, Ph.D. diss. Stockholm: Department of Computer and Systems Sciences, Stockholm University and Royal Institute of Technology. 94:004.

Labuschagne, L. 2001 Web Assurance: Information security management for e-commerce. In *Advances in Information Security Management & Small Systems Security, Proceedings of the eighth annual working conference of WG 11.1 and 11.2 of technical committee 11 part of International federation for information processing, held in Las Vegas 27-28 September 2001 (conference was postponed due to the September 11 terrorist attacks in the USA)*, edited by Eloff, J.H.P., L. Labuschagne, R. von Solms and G. Dhillon, Boston: Kluwer Academic Publishers.

Liebenau, J., and J. Backhouse. 1990. *Understanding Information: An Introduction.* London: Macmillan Press.

Lincoln, Y.S. and E.G. Guba. 1985. *Naturalistic inquiry.* Beverly Hills, CA: Sage.

Marin, A. 1992. Cost and benefits of risk reduction. In *Risk: Analysis, perception and management.* London: Royal Society.

Miller, J.G. 1978. *Living Systems.* McGraw Hill.

Mintzberg, H. 1983. *Structures in Fives: Designing Effective Organizations.* Englewood Cliffs: Prentice-Hall.

Morris, C. 1938. *Foundations of the Theory of Signs.* Chicago: University of Chicago Press.

Murray, W. 1995. Security Should Pay: It Should Not Cost. In *Information Security - the Next Decade, Proceedings of the IFIP TC11 11th annual working conference on information security*, edited by Yngström, L. Amsterdam: Kluwer Academic Publishers.

NIST Common Criteria Project. 1997. *The Common Methodology for Information Technology Security Evaluation, CEM-97/017.* Available online from http://csrc.nist.gov/cc/cem/cemlist.htm. Accessed 2001-10-24

NIST (National Institute of Standards and Technology). 1998. *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, by Wilson, M., D. Zafra, S. Picher, J. Tressler, and J. Ippolito, 16 April 1998, NIST SP-800-16. Gaithersburg: National Institute of Standards and Technology.

Owens, S. 1998. *Information Security Management - An Introduction*, London: British Standards Institute.

Parker, D.B. 1995. A New Framework for Information Security to Avoid Information Anarchy. In *Information Security - the Next Decade, Proceedings of the IFIP TC11 11th annual working conference on information security*, edited by Yngström, L. Amsterdam: Kluwer Academic Publishers.

_____. 1997. The Strategic Values of Information Security in Business. *Journal of Computers & Security* 16: 572-582.

Qing, S., and J. Eloff. 2000a. *IFIP/SEC2000: Information Security – Information Security for Global Information Infrastructures, Proceedings of the IFIP TC11 16th annual working conference on information* held in Beijing during the World Computer Congress, August 21-25 2000. Beijing: International Academic Publishers.

_____. 2000b *Information Security for Global Information Infrastructures, Proceedings of the IFIP TC11 16th annual working conference on information security,* held in Beijing during the World Computer Congress, August 21-25 2000. Amsterdam: Kluwer Academic Publishers.

Riksrevisionsverket. 1997. *Datorrelaterade missbruk och brott - en kartläggning gjord av effektivitetsrevisionen.* Stockholm: Riksrevisionsverket. 1997:33.

Rapoport, R.N. 1970. Three Dilemmas in Action Research. *Human Relations* 23, no. 4: 1970: 499-513.

Simon, H.A. 1948. *Administrative Behaviour.* New York: Macmillan.

Siponen, M. 2001. On the scientific background of information security management standards: a critique and an agenda for further development. In *Proceedings of the Second Annual Systems Security Engineering Conference (SSE), held in Orlando 28 February - 2 March 2001.*

SIPS (Swedish Information Processing Society). 2001a. *Web site http://www.dfs.se/products/sbaeng/ for product information and evaluation copy in English.* Accessed 2001-09-15. Stockholm: Swedish Information Processing Society.

_____. 2001b. *SBA Scenario - Metod- och programbeskrivning.* Available online from http://www.dfs.se/products/sba/scenario/smetod.asp. Accessed 2001-10-24. Stockholm: Swedish Information Processing Society.

SIS (Swedish Standards Institute). 1999a. *Ledningssystem för informationssälkerhet – Del 1: Riktlinjer för ledning av informationssäkerhet (Svensk standard SS 62 77 99-1).* Stockholm: SIS Förlag AB.

_____. 1999b. *Ledningssystem för informationssälkerhet – Del 2: Specifikation för ledningssystem för informationssäkerhet (Svensk standard SS 62 77 99-2).* Stockholm: SIS Förlag AB.

_____. 2001. *Ledningssystem för informationssälkerhet – Del 1: Riktlinjer för ledning av informationssäkerhet (Svensk standard SS-ISO/IEC 17799).* Stockholm: SIS Förlag AB.

SSE-CMM Project. 1999. *Systems Security Engineering Capability Maturity Model. Model Description, Version 2.0.* Available online from http://www.sse-cmm.org. Accessed 2001-10-24. Vienna, VA.: SSE-CMM Project.

Stamper, R., K. Liu, M. Kolkman, P. Klarenberg, F. Van Slooten, Y Ades, and C. Van Slooten. 1991. From Database to Normbase. *International Journal of Information Management* 11: 67-84.

Strauss, A. and J. Corbin. 1994. Grounded Theory Methodology – An Overview. In *Handbook of Qualitative Research*, ed. Denzin and Lincoln, 273-285. London: Sage Publications.

Susman, G. and R. Evered. 1978. An assessment of the scientific merits of action research. *Administrative Science Quarterly* 23, no. 4: 582-603.

Von Solms, R. 1999. Information security management: Why standards are important. Information Management and Computer Security 1, no. 7.

Von Solms, S. 2000. Information Security - The Third Wave?. *Journal of Computers & Security* 19, no. 7: 615-620.

Warren, M.J., S.M. Furnell and P.W. Sanders. 1997. ODESSA - A new approach to healthcare risk analysis, in *Information Security in Research and Business, proceedings of the thirteenth international conference on information*

security, edited by Yngström, L. and J. Carlsen, 391-402. London: Chapman & Hall.

Yngström, L. 1983. Education in Safety Systems and Security Analysis - Suggestions for a One Year University Program. In *Proceedings of the IFIP TC11 first working conference on information security held in Stockholm.*

_____. 1988. Experiences from a one-year Academic Programme in Security Informatics. In *Proceedings of the Fifth International Conference on Computer and Security held in Queensland Australia* 1988.

_____. 1989. Experiences from a one-year Academic Programme in Security Informatics. *Information Age* 11: 77-82.

_____. 1991. *Security Informatics 1985-1991: An assessment.* Stockholm: Department of Computer and Systems Sciences, Stockholm University and Royal Institute of Technology. SIIS-R-91.

_____. 1993. Evaluation of an academic programme in IT Security 1985-1990. In *Computer Security: Discovering Tomorrow, Proceedings of the IFIP TC11 9th annual working conference on information security.*

_____. 1996. *A systemic-holistic approach to academic programmes in IT security*, Ph.D. diss. Stockholm: Department of Computer and Systems Sciences, Stockholm University and Royal Institute of Technology. 96:021.

Yngström, L. and F. Björck. 1998. The Value and Assessment of Information Security Education and Training. In *WISE 1, Proceedings of the IFIP TC11 WG 11.8 First World Conference on Information Security Education, held in Stockholm June 17-19.* edited by Yngström, L. and S. Fischer-Hübner, 271-292. Stockholm, Sweden: International Federation for Information Processing.

8. APPENDIX A – PAPER D: "IFIP WORLD COMPUTER CONGRESS (SEC 2000) REVISITED"

This paper introduces a simple classification model for research in information security[1]*. The level of abstraction ('theories and models', 'empirical world') and domain (technical, formal, informal) are proposed as the key dimensions in the model. The 125 papers selected by international reviewers for presentation and publication at the IFIP World Computer Congress / SEC 2000 were analysed and classified according to the model, and the outcome of this effort is presented. The result is a high-level graphical view of what type of research that was presented in the SEC 2000 proceedings and at the conference in Beijing. Finally, we discuss the content of the congress with this view as our point of departure, aiming to identify areas that are well covered as well as areas that leave room for further advancement. As an appendix in this thesis, the paper serves two purposes: One, it illustrates the current trends and foci in information security research in a global context. Two, it shows that the subject tackled in this thesis – the management of information security in organisations – needs to be further investigated and researched.*

8.1 The Model

Research in information security encompasses many different disciplines[2], competencies and focal points[3]. Moreover, it is of course possible to view the information security area from many different perspectives. Logically, the classification model presented here only represents one of innumerable potential views (figure 8.1). The purpose of this model is to facilitate the analysis of research in information security, by - for a given paper (or other research contribution) - showing the type of research reported on and within which domain it is positioned. The following sub-sections present the model, its origins and application in more detail.

[1] This chapter is based on a previously published research paper (Björck and Yngström 2001)

[2] Research in information security is carried out within the boundaries of many (reference) disciplines such as mathematics, computer science, social psychology, information science, criminology, etc.

[3] For example, some researchers in information security focus on computer systems, some on human activity systems, and others on privacy implications of information technology, etc.

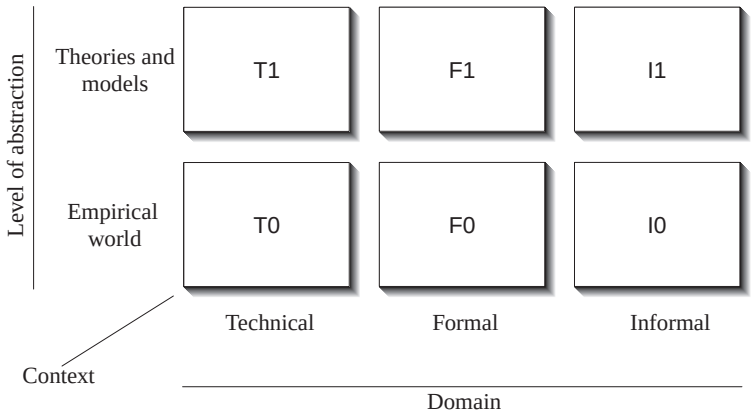


Fig. 8.1: *A classification model for information security research.*

8.1.1 Dimension X: Level of abstraction

This first dimension, ranging from *theories and models* to *empirical world*, caters for the need to distinguish between what is real, and what is not. For example, the well-known Bell-LaPadula model specifies a multi-level security policy for a military computer system using mathematical notation and set theory (Bell and LaPadula 1974). This model is an idea, a model, and a basic security theorem, specifically concerned with the security of a technical system, and it would therefore be positioned in the T1 quadrant in the classification model proposed here (figure 8.1). An existing access control system that *implements* the Bell-LaPadula model would be found in the empirical world, in the T0 quadrant in the classification model. Other models represent similar - but not necessarily identical - dimensions of information security with concepts such as:

- *Systems thinking* (models an ideal situation) and *real world thinking* offered by Soft Systems Methodology (Checkland 1981), used in the area of information security by for example Fillery-James (1999).
- *Design/architecture*, *theory/model*, and *physical construction*, offered by General Living Systems Theory (Miller 1978), used in the area of information security by Yngström (1996).

Focusing the variation in the level of abstraction is essential, since it helps us not only to detect if a given text reports on an idea, theory or model, or if it is concerned with artefacts in the physical world, but more importantly, it helps us to see clearly if any attempts were made move up or down in this dimension. In the case of the Bell-LaPadula model, used in the previous example, the process of implementing the model in a computer based access control system may be described as a deductive undertaking. Such a process can be represented in the

classification model as an arrow from T1 to T0. Likewise, an inductive process can be illustrated with an arrow going in the other direction[4].

8.1.2 Dimension Y: Domain

The *domain* dimension, ranging from *technical*, via *formal* to *informal*, originates from the work of Stamper *et al.* (1991)[5]. Other models represent a similar – but again, not necessarily identical - dimension of information and security with concepts such as:

- *Technical*, *operational*, *managerial*, *legal*, and *ethical* in the Systemic-Holistic Model by Yngström (1996).
- *Hardware*, *operating system*, *application*, *operational*, *administrative/managerial*, *political/legal*, and *ethical* in the Security By Consensus Model by Kowalski (1994).
- *Empirics*, *syntactics*, *semantics*, *pragmatics*, and *social world*. The three middle concepts are taken from the field of semiotics, originally introduced by Morris (1938). The two additional ones have later been proposed and described by a number of authors, for example Liebenau and Backhouse (1990).

The *technical* domain in the classification model (T0, T1) encompasses technical artefacts or ideas, models and theories about these (depending on the *level of abstraction*). Examples:

1. computer hardware and software,
2. communication protocols and cryptographic algorithms,
3. technical evaluation methodologies,
4. *etc.*

The *formal* domain in the classification model (F0, F1) encompasses formal rules and procedures used to formalise human behaviour in an information system. *Formal* are those rules or procedures that are made explicit (usually - but not necessarily – *written*)[6]. Examples:

[4] Instantly recognisable deductive and/or inductive research approaches in information security might be relatively difficult to find. On the other hand, the model can be used also to illustrate the absence or combination of these and other research approaches.

[5] Dr. James Backhouse at the Computer Security Research Centre at the London School of Economics introduced these concepts (*technical*, *formal* and *informal*) and their usefulness within information systems security to the author in 1996.

[6] Some might argue that software (such as operating systems, communication protocols, and applications) should be positioned in this *formal* domain, since they in fact consist of a set of formalised rules (the code). However, for the purpose of the proposed classification model in this paper, we have made the choice to distinguish between rules and procedures designed for humans and those designed for non-human processors, such as a CPU in a computer system. Thus, the formal domain only encompassed rules and procedures aimed at a human receiver.

1. organisational information security policy,
2. legal system,
3. formal decision hierarchies,
4. *etc.*

Consequently, the *informal* domain in the classification model (I0, I1) encompasses informal human behaviour or ideas, models and theories about these. Examples:

1. social relations,
2. security implications of casual interpersonal communication,
3. ethics,
4. factual (as opposed to formal) organisational structures,
5. power struggles,
6. *etc.*

By introducing this dimension, the classification model becomes more focused on research in information security within an organisational context. This may perhaps be an advantage, since it is in this setting that most information security services and products are demanded and will be used.

8.1.3 Dimension Z: Context

Context is added as a third dimension. Here, it originates from the systemic-holistic model (Yngström 1996) where this factor is offered to cater for time and space. To continue the same example; the Bell-LaPadula model was presented in 1974 (time). It was concerned with the security of computer systems in a military setting (space).

This concludes the presentation of the classification model. Advantages and disadvantages of the proposed model are not further discussed in this paper. Nevertheless, some of these issues will most likely become apparent to the reader as we move on to applying the model in practice.

8.2 The Approach

The 125 papers from the IFIP World Computer Congress / SEC 2000 (Qing and Eloff 2000a, 2000b) were analysed and classified according to the classification model proposed here.

This is a step-by-step description of how the examination and classification was approached:

```
1.Read all papers one by one and
     a)extract and record the main focus,
     b)extract and record the main contribution, and
     c)make a preliminary classification according to the model.

2.Read all papers for a second time and
     a)extract and record the type of contribution,
     b)note type of test or validation if performed, and
     c)note if evaluation results were presented.

3.Make a definitive classification according to the model.
```

The results were recorded in a simple spreadsheet to facilitate the awaiting statistical analysis.

Some of the information collected in the approach described above does not intuitively fit into the proposed classification model. Nevertheless, this information is needed for two reasons: Firstly, to more exactly decide on the position of the paper in the model (for example within a quadrant), and secondly, to detect if attempts are made at "moving around" in the model (for example; "Is this proposed technical computer system (quadrant T1) tested in a real-world setting (quadrant T0)?").

There were no restrictions on the number of categories for the type of contribution or the type of test. However, after all papers were analysed, there were still no more than 12 *types of* research contributions and 6 *types of* tests recorded. Of course, if we had preferred - and actively sought after – more narrow groupings, the effect would have been a more precise result, but also more categories.

8.3 The Result

First, a high-level view - using the proposed classification model (figure 8.2) - of the 125 papers from the IFIP World Computer Congress / SEC 2000 (Qing and Eloff 2000a, 2000b): Each dot in the figure represents one of the 125 papers. All dots that are positioned between an upper and a lower quadrant (within the dotted line) are those that involve some kind of movement in terms of level of abstraction (for example, testing a suggested approach by implementing it). Arrows indicating the correct direction should ideally have represented these papers, but due to space restrictions they are shown as dots here.

As can be deduced from studying the results shown in the classification model above, circa 104 of the 125 papers, or 83%, were of a technical nature, 14% of a formal and 3% of an informal nature (please refer to the section describing the classification model, 8.1, for a clarification of the concepts; technical, formal and informal). See figure 8.3. That was the results from the horizontal analysis using the model. Let us examine the model vertically instead (results presented in figure 8.4 below). Again, the 25% "Moving" papers are those that involve some kind of movement in terms of level of abstraction (for example, testing a suggested approach by implementing it). The remaining papers, in total

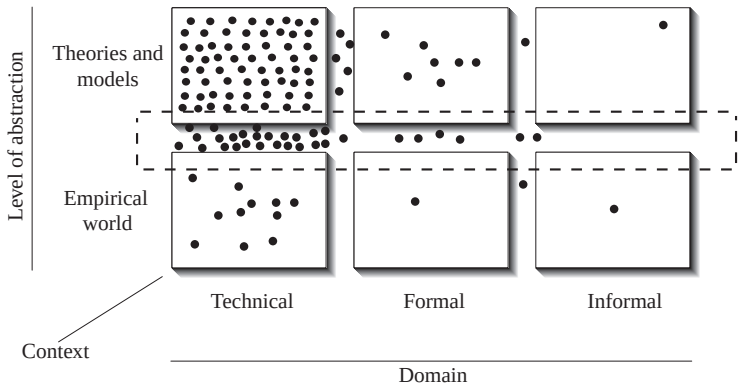


Fig. 8.2: *Applying the classification model to the 125 papers from the SEC 2000 proceedings.*

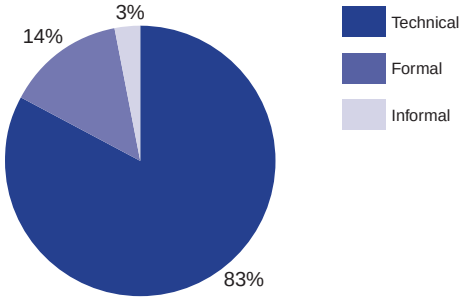


Fig. 8.3: *SEC 2000; proportions of research papers in each domain.*

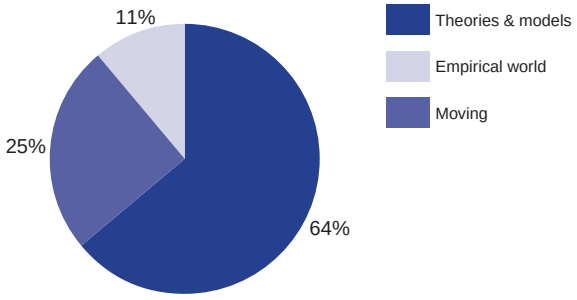


Fig. 8.4: *SEC 2000; proportions of research papers at different levels of abstraction.*

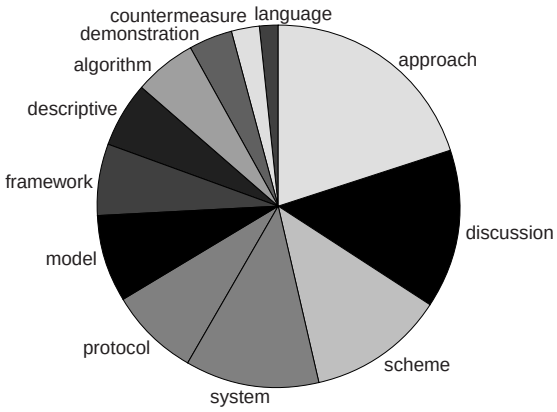


Fig. 8.5: *SEC 2000; types of contribution.*

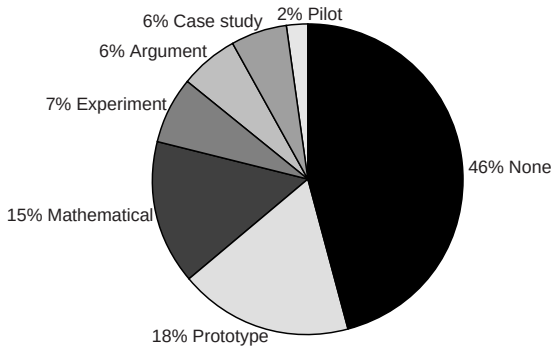


Fig. 8.6: *SEC 2000; types of tests.*

75%, did not describe any such movements (figure 8.4). *The most common type of contribution was described as an approach* (20%), followed by *discussion* (14%), *system* (12%) and *scheme* (12%)[7]. In total, almost 6 out of 10 papers' contributions were of one of these four types (figure 8.5).

Nearly half of the papers (46%) did not describe any tests *vis-à-vis* their conclusions. 18% tested the soundness of their findings by using a *prototype*, and 15% by means of mathematical proof (figure 8.6). This means that; of the 66 papers that reported some sort of test, more then 6 out of 10 used either a prototype or mathematics to test their results.

Even though about 46% declared that they employed some kind of test (figure 8.6), only 14% of the 125 papers presented evaluation results (qualitative or quantitative) from such tests, as shown in figure 8.7

[7] This information cannot be derived from studying the results in the classification model, please refer to the section in this paper describing the research approach for more information.

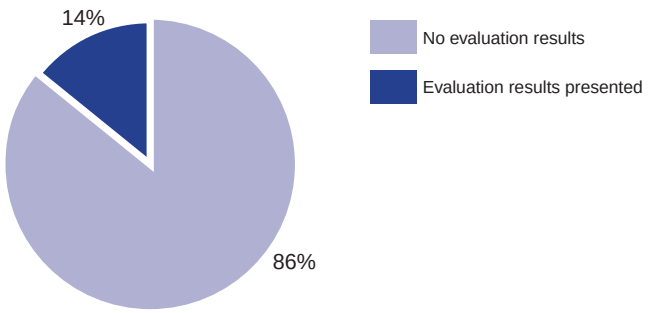


Fig. 8.7: *SEC 2000; proportion of papers that contain evaluation results.*

1	Employee awareness	33,80%
2	Budget	27,10%
3	Human resources	25,40%
4	Management support	18,90%
5	Tools/security solutions	17,90%

Fig. 8.8: *Greatest obstacles to addressing security concerns*

8.4 The Discussion

More than 8 out of 10 analysed papers are focusing on technical issues, even though research and practical experience confirms that human behaviour - as represented by the formal and *informal* domains in the proposed model - largely affect the success of information security.

For example, a survey on computer crime, based on answers from 1304 organisations with over 50 employees in Sweden found that employees' information security awareness is perceived as *the most important* means to overcome the security problems (Riksrevisionsverket 1997). Another study, based on a survey about threats to EDP-stored information answered by 162 IT-managers, concluded, "The respondents consider the main threat against the organisations' EDP stored information to be employees' unintentional and erroneous change and deletion" (Johansson and Kager 1995). The result from Ernst & Young's Annual Global Information Security Survey (Ernst & Young 1999), based on responses from over 4300 IT and executive managers in 35 countries, further underscores this line of reasoning (figure 8.8).

The question was "Which of the following is the greatest obstacle to addressing security concerns?" Of the five obstacles listed in the survey questionnaires, tools and technical security solutions were seen as the least significant obstacle, while employee awareness was seen as the primary challenge.

As mentioned, the analysis showed that more then 8 of 10 papers were focusing on technical issues. Technically oriented security research (and solutions) is crucial, since it lays the foundation to the secure operation of information and communication technologies. But today, as now evident, the critical problem is

to be found elsewhere – in the *formal* and *informal* domains of the classification model.

8.5 The End

The main contribution of this paper was to propose a classification model for information security research. This model was subsequently applied to the 125 papers published in the proceedings of the IFIP World Computer Congress / SEC 2000. The main result of this analysis was the identification of an inconsistency between the current problems regarding information security in organisations today on the one hand, and the focus of the 125 presented papers on the other hand. This outcome suggests that more emphasis should be placed on research on issues in the formal and *informal* domains such as information security education, the management of information security, ethics in information security, information security management systems, information security awareness and information security policies.

9. APPENDIX B: ”REVISORERNA OM INFÖRANDE OCH CERTIFIERING AV LIS”

9.1 Bakgrund

På uppdrag av SIS' LIS-projekt har Institutionen för Data- och Systemvetenskap vid Stockholm Universitet / KTH genomfört en kvalitativ enkätstudie syftande till att identifiera de erfarenheter och insikter deltagarna i projektets arbetsgrupp 3 erhållit beträffande införande och certifiering av ledningssystem för informationssäkerhet, LIS [1]

Genom att möjliggöra samarbete mellan informationssäkerhetskonsulter, revisorer, myndigheter (främst SWEDAC), och organisationer som söker certifiering, har arbetsgruppen sökt skapa och dokumentera unika erfarenheter. Syftet med denna rapport är att kommunicera dessa erfarenheter både inom och utom projekt LIS. Det torde finnas ett mycket stort intresse för detta, inte minst med tanke på att standarden nyligen blivit antagen av ISO som en internationellt erkänd standard, då med beteckningen ISO/IEC 17799:2000 (ISO 2000).

Certifieringsrevisorernas och informationssäkerhetskonsulternas erfarenheter och insikter studerades i två separata studier. *Denna rapport beskriver endast resultatet från studien av revisorerna. Det finns en motsvarande rapport om konsulternas erfarenheter.*

I december 2000 nåddes en mycket viktig milstolpe för arbetsgruppen i och med att en av pilotorganisationerna blev tredjepartscertifierade enligt standarden. Därmed övergick arbetsgruppens fokus från att genomföra pilotcertifieringar till att dela med sig av alla de erfarenheter som skapats under de gångna åren. Denna studie och rapport är ett led i detta arbete.

9.2 Metod, demografi och reliabilitet

Undersökningen genomfördes som en skriftlig enkätundersökning med öppna frågor. Enkäten skickades ut till samtliga revisorer som deltagit i ”pilotpro-

[1] Originalrapportens titel är ”Certifieringsrevisorernas perspektiv på införande och certifiering av LIS – en enkätundersökning”. Undersökning och rapport av Fredrik Björck som observatör i Projekt TK 099 ”Ledningssystem för Informationssäkerhet, LIS”, Arbetsgrupp 3 ”Pilotprojektet” (numera ”7799.nu”), SIS Standardisering i Sverige.

jektet" (AG3) inom standardiseringsgruppens (STG) projekt TK099 – Ledningssystem för informationssäkerhet. Totalt kontaktades åtta respondenter med enkäten (*n=8*), och antalet svar efter *en* påminnelse slutade på sex, vilket ger en smått imponerande svarsfrekvens på 75% (*(6/8)*100*).

Generalisering utifrån resultatet är inte nödvändig, då det inte finns någon bakomliggande population vi önskar dra slutsatser mot. Undersökningen skall ses som ett försök till kartläggning av unika erfarenheter hos de personer som deltagit i ovan nämnda pilotprojekt. Det är således fråga om en totalundersökning av den föreliggande populationen.

Samtliga respondenter har mycket gedigen erfarenhet av certifiering, och 83% av dem var direkt involverade i en eller flera av de organisationer som sökt nå certifiering enligt 7799 (SIS 1999b) genom pilotprojektet. De tillfrågade lovades anonymitet i följebrevet.

Vid några få tillfällen har svaren ändrats marginellt för att korrigera ett stavfel eller en grammatisk miss, eller för att förtydliga innebörden (ex. "enhet" har ändrats till "organisatorisk enhet"). Dessa ändringar har genomförts med stor försiktighet så att svarets semantiska innehåll inte har ändrats, utan snarare förtydligats.

Slutsatserna bygger på en strukturerad analys av det kvalitativa datamaterial svaren sammantaget utgör. Eftersom svaren samlats in elektroniskt från respondenterna minimeras de fel som annars ofta uppkommer vid inmatning på grund av överföring från ett media till ett annat (ex. vid avskrift av ljudupptagning för senare analys). Analysen av datamaterialet gick till så att varje svar (eller till och med *del* av ett svar) kodades med en kod som angav dess innehåll. Respondenternas olika svar på en given fråga (kontext) relaterades sedan till varandra med hjälp av koderna. Sakta växer då en modell (i det här fallet en visuell nätverksmodell) fram som visar likheter och skillnader i svar, samt som får oss att fokusera på det viktiga i svaren. Analysarbetet och den därpå följande induktiva processen (från enskilt svar via svarsmönster till slutsatser) underlättades av ett datoriserat metodstöd (ATLAS.ti), vilket gör det möjligt för andra att i efterhand kontrollera rimligheten i slutsatserna genom att undersöka vad – exakt vilka uttalanden/svar – respektive slutsats bygger på. En översiktsskiss som demonstrerar detta återfinns i slutet av rapporten.

Det har inte varit svårt att hitta gemensamma nämnare och mönster i svaren trots det låga antalet personer som deltagit i studien – tvärtom! Materialet visar på en närmast ofattbar samstämmighet, vilket ytterligare förvissar oss om att slutsatserna i föreliggande rapport är korrekta. Med korrekt skall förstås att; rapporten ger en riktig bild av hur de tillfrågade svenska revisorerna ser på de undersökta aspekterna beträffande införande och certifiering av ledningssystem för informationssäkerhet enligt 7799 (SIS 1999b).

9.3 Framgångsfaktorer för införande

Den första frågan i enkäten till revisorerna löd:

> *Vad anser Du vara de viktigaste faktorerna för ett framgångsrikt införande av ett ledningssystem för informationssäkerhet, LIS? (motivera gärna svar)*

Ur svaren växte ganska omgående sex olika framgångfaktorer fram. Eftersom samstämmigheten var så god väljer vi här att presentera svaren ordnade efter respektive faktor – i fallande ordning med den viktigaste, eller i vart fall den mest frekvent nämnda, faktorn först. Det kan vara värt att nämna att samtliga svar – hela materialet – föll under dessa sex faktorer utan ansträngning.

Framgångsfaktorer vid införande av LIS, ur revisorernas perspektiv, är följande:

9.3.1 Ledningens engagemang

Förankring i organisationens ledning, samt ledningens engagemang och förståelse för informationssäkerhetsproblematiken ansågs som den viktigaste faktorn för ett framgångsrikt införande av LIS. Denna faktor angavs först av samtliga, fastän enkäten inte hade några svarsalternativ och trots att respondenterna svarat ovetandes om de andras svar. Följande citat talar för sig själva:

> *”Ledningens intresse och aktiva engagemang i det egna LIS-projektet....”*
>
> *”Ledningens engagemang och en förståelse för att ledningssystemet för informationssäkerhet måste omfatta hela verksamheten.”*
>
> *”Ledningens engagemang...”*
>
> *‘”Ledningens förståelse och engagemang, både i samband med fastställandet av säkerhetspolicy / säkerhetsnivå och att delta aktivt i riskbedömningen och avbrottsplaneringen.”*
>
> *”Företagsledningens engagemang....”*
>
> *”Förankring i företagets/organisationens ledning....”*

9.3.2 Välstrukturerat projekt

En annan viktig framgångsfaktor som identifierades är att projektet som skall införa LIS i organisationen är väl planerat och strukturerat. De olika respondenterna utrycker sig så här:

> *”En organisatorisk enhet som ansvarar för helheten och för den riskanalys om ligger till grund för allt arbete....”*
>
> *”...ett väldefinierat projekt med avgränsade delprojekt....”*
>
> *Väl utarbetad projektplan och en rätt dimensionerad projektorganisation....”*

Sammantaget är det flera olika aspekter rörande just organiseringen av själva arbetet med att skapa och införa ett LIS som tas upp:

- att helhetsansvaret för projektet är definerat,
- att det står klart *vem* som skall genomgöra de olika delstegen i projektet
- att mål, medel och tidsplan för projektet är utarbetat och dokumenterat i en projektbeskrivning eller motsvarande, samt
- att resurserna i projektet – inte minst de mänskliga – är väl avvägda.

9.3.3 Holistiskt angreppssätt

Projektmedlemmarnas - och de övriga medarbetarnas - förmåga att se helheten betonas av flera av de tillfrågade som en viktig framgångsfaktor. Det verkar bland revisorerna finnas en känsla av att de datatekniska aspekterna ofta hanteras ganska detaljerat, men på bekostnad av helhetssynen. Därför menar de att ett mer holistiskt angreppssätt och tänkande i projekten skulle medföra positiva konsekvenser och bereda väg för en framgångsrik implementering och eventuellt därpå följande certifiering av LIS. Två av de tillfrågade utrycker det på följande sätt:

> *”...att de som deltar i arbetet med att ta fram risker är representatnter för hela företaget, alltså inte bara för säkerhet utan även för andra delar av verksamehten.”*
>
> *”förståelse för att ledningssystemet för informationssäkerhet måste omfatta hela verksamheten”*

Som framgår av citaten är det främst kopplingen mellan informationssäkerheten och organisationernas kärnverksamheter som anses som viktigt – att LIS tar i beaktande och omfattar hela verksamheten – så att det inte stannar på säkerhets- eller IT-avdelningen.

9.3.4 Insikt om behov av informationssäkerhet

Att organisationerna inser behovet av informationssäkerhet är ytterligare en framgångsfaktor som identifierades:

> *”...att företaget ser ett behov av att skydda sin egen, kunders och andra intressenters information.”*
>
> *”...förståelse för att ledningssystemet för informationssäkerhet måste omfatta hela verksamheten”*
>
> *”Ledningens förståelse...”*

Denna framgångsfaktor kan kanske anses som självklar. Trots detta nämns den vid flera tillfällen av de tillfrågade. Kanske indikerar detta att man ibland upplever en bristande förståelse avseende vikten av informationssäkerhet från delar av organisationen – kanske inte minst ledningsgrupperna.

9.3.5 Motiverade medarbetare

Några av delsvaren fokuserar på behovet av att motivera medarbetare:

> *"Att motivera de anställda till att arbeta fram processer och rutiner inom deras egna ansvarsområden...."*
>
> *"...engagerad projektledare /-deltagare...."*

Svaren tar främst upp vikten av att motivera personer som deltar i själva LIS-projekten, såsom projektdeltagare, projektledare, och ansvariga för olika delverksamheter i organisationen. Efter det att LIS skapats måste det också införas, och i det skeded växer vikten av denna framgångsfaktor – då skall *alla* medarbetare i hela organisationen motiveras att följa de regler och dagligen använda de tekniska lösningar projekten tagit fram och ledningen sedan beslutat.

9.3.6 Tillgång till extern kompetens

Den sista framgångsfaktorn som fångades upp i enkäten var just vikten av att kunna ta in extern kompetens där så krävdes:

> *"...bra bollplank (gärna certifieringsorgan från början)."*
>
> *"... Tillgång till extern specialistkunskap."*

Det handlar då både om specialister och rådgivare inom informations- och IT-säkerhet, men även om att redan i ett tidigt skede öppna för en dialog mellan organisationen och certifieringsorgan. Denna kontakt – organisation *vs.* certifieringsorgan - måste ses som mycket viktig – inte minst om organisationen planerat att söka certifiering av sitt LIS efter införandet.

9.3.7 Sammanfattning

Genom analys av den kvalitativa enkätundersökningens svar från certifieringsrevisorerna inom projektet LIS, identifierades sex stycken framgångsfaktorer med avseende på framgångsrikt införande av ett ledningssystem för informationssäkerhet. Eftersom certifieringsrevisorernas roll främst är att i efterhand kontrollera om ett ledningssystem för informationssäkerhet lever upp till kraven i standarden (SIS 1999b), så är deras perspektiv en framförallt en betraktares, snarare än en utförares. Figuren ger en sammanfattande bild av certifieringsrevisorernas svar (figur 10.1):

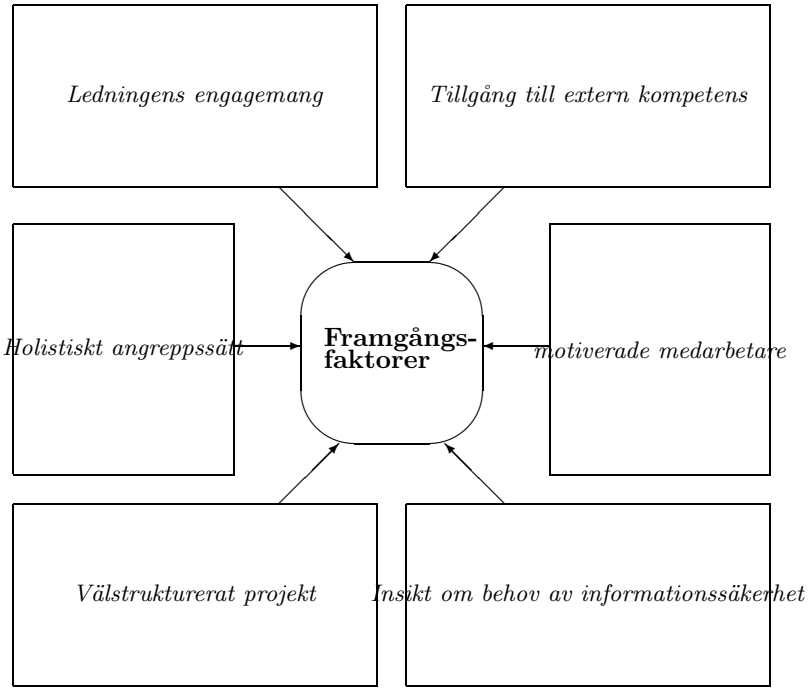


Fig. 9.1: *Framgångsfaktorer för lyckat införande och certifiering av ledningssystem för informationssäkerhet enligt SIS (1999b), ur certifieringsrevisorernas perspektiv.*

9.4 Svårigheter och utmaningar vid certifiering av LIS

Den andra frågan i enkäten till revisorerna löd:

> *Vad anser Du vara de största utmaningarna när det gäller certifiering av LIS enligt SS627799? (motivera gärna svar)*

("SS627799" i frågan åsyftar standarden som återfinns under referens SIS (1999b) i referenslistan – det är den officiella svenska beteckningen på certifieringsdelen av standarden som brukar kallas "7799")

Ett utdrag av svaren:

> *"Utmaningen ligger inte i certifieringen utan i införsäljningen av budskapet att det är nödvändigt med en tredjepartsbedömning för att inte bli hemmablind!"*
>
> *"Att få företagen att tänka över vilken information de behöver skydda. Viss information kan säkert "läcka" utan att skada företaget."*
>
> *"Att få en förståelse för att ledningssystemet för informationssäkerhet skall omfatta hela verksamheten. Detta är svårt för många och visar sig exempelvis i samband med riskanalys, avbrottsplanering och i planering för incidenthantering."*
>
> *"Att se till helheten och förstå att det inte bara gäller IT utan till stor del andra delar det vill säga personal, skalskydd, etc. Att säkerställa att riskanalysen görs på ett för företaget korrekt sätt och att applicera den till företagets behov och utveckling, samt att den blir heltäckande."*

Svaren kan hänföras till tre olika problemtyper;

- ett *pedagogiskt* problem; hur *förklara* att LIS gäller hela verksamheten?,
- ett *marknadsföringsmässigt* problem; hur *övertyga* att certifering ger mervärde?
- ch slutligen ett *metodrelaterat* problem; hur *säkerställa* att korrekt riskanalys genomförts?

Som en konsekvens av hur frågan är ställd ger egentligen svaren på frågorna inga svar – utan bara ytterligare frågor som kan, och kanske bör, tas upp för ytterligare diskussion. Här är en början på en diskussion kring de tre identifierade problemtyperna:

9.4.1 Overtyga att certifering ger mervärde

Att låta tredje part intyga att ett LIS är effektivt och lever upp till kraven i 7799 (SIS 1999b) kan medföra flera fördelar för en organisation. Problemet

är att dessa fördelar inte nödvändigtvis gör sig tydliga för organisationen av sig själva. De kan se det så här: Om LIS redan är infört och om det redan fungerar, vilket är förutsättningen för en certifiering, så är ju redan informationssäkerheten god. Givetvis medför varje certifiering att problem upptäcks och kan åtgärdas, vilket i praktiken höjer informationssäkerheten. Om en höjning av informationssäkerheten är det *enda* som önskas torde dock en certifiering som åtgärd vara ganska dyrbar jämfört med en snabb nulägesanalys (med därpå följande åtgärder) av informationssäkerheten med hjälp av en informationssäkerhetsspecialist. Värdet av en certifiering blir således, ur detta perspektiv sett, främst att en oberoende tredje part intygar att LIS är implementerat, fungerar effektivt, och att det lever upp till kraven i 7799 (SIS 1999b). Eftersom tjänsten – certifiering – främst är en försäkran för affärspartners och medarbetare, så är värdet av denna avhängigt *deras uppfattning* av värdet av ett sådant intygande. Denna uppfattning kommer att avgöras av hur skickliga certifieringsorganen är på att utföra certifieringarna, samt deras förmåga att kommunicera certifieringens fördelar för andra organisationer. Man kan också se det som självklart att en certifiering medför ett mervärde i och med att andra parter kan lita på att vissa krav efterlevs. Detta synsätt förutsätter att det finns en någorlunda gemensam tolkning av standardens styrmedel och formkrav. Som sagt, frågan löses inte här – vi kan bara kontatera att detta är en av de utmaningar revisorerna ser.

9.4.2 Säkerställa att korrekt riskanalys genomförts

Revisorerna kommer ofta in i ett ganska sent skede – när LIS redan är infört. Detta gör att de genom att granska dokument från riskanalysprocessen måste kunna bilda sig en uppfattning av hur riskanalysen gick till och om den varit adekvat. Svårigheten ligger i att avgöra huruvida en given analys verkligen var fullgod, eller om det endast var rapporten om den som var välskriven. Omvänt gäller också att riskanalysen kan ha varit mycket effektiv, medans dess process och resultat av någon anledning blivit sämre dokumenterat. Sammanfattningsvis; utmangingen för revisorerna ligger i *att i efterhand säkerställa* att en korrekt och adekvat analys genomförts.

9.4.3 Förklara att LIS gäller hela verksamheten

Den sista gruppen av delsvar gäller det vi här valt att kalla den pedagogiska utmaningen; att förklara för personer i organisationerna att LIS gäller hela verksamhetens informationshantering och inte bara exempelvis den databurna informationen. Detta framkommer dessutom i svaren på såväl den första som den kommande frågan.

9.5 Fokus och tyngdpunkter i LIS-projekt

Den tredje frågan i enkäten till revisorerna löd:

> *Tycker Du att det (i det 7799-projekt Du tänker på eller generellt) funnits en bra balans vad avser fokus på datateknik-organisation, verklighetdokument, produktivitet-säkerhet (eller andra dimensioner)? Finns det delar som överfokuserats eller aspekter som fokuserats för lite? (förklara gärna svar)*

Ett utdrag av svaren:

> *"Bra i projektet men generellt tror jag att det finns en överfixering mot dataproblematiken, vilket gör att man missar delar av det övriga. Motmedel: följ standarden och skapa checklistor."*
>
> *"I det projekt som jag var involverad i var det huvudsakliga problemet att man bokstavligen läste standarden innantill och trodde att man var tvungen att uppfylla varje punkt utan att hänsyn till företagets behov (exempelvis med få lap-tops i företaget och inget behov att ta ut dem, så fanns det för närvarande inget behov av kryptering av hårddiskarna."*
>
> *"För mycket teknikorienterat. En tydligare fokus borde vara på helhetstänkande."*
>
> *"För lite fokus på affärsnytta, system och helhetstänkande och för mycket fokus på tekniska aspekter och nästan bokstavstrogen anpassning till standardens (del 1 av 7799) erfarenheter och förslag till styrmedel."*
>
> *"Generellt anser jag att de pilotföretag jag mött varit fokuserade på IT-säkerhetsperspektivet och inte på ledningssystemperspektivet och det vidare informationssäkerhetsperspektivet."*
>
> *"Vid våra sammanträden har ibland rena IT-frågor fått större vikt än övrig information. Under senare tid har mitt deltagande i sammanträdena och projektet varit begränsat."*

Analys av svaren ger vid handen att det främst är två skiften i fokus som önskas, sett ur revisorernas synvinkel:

- *Från* IT-fokusering *till* en helhetssyn på säker informationshantering, och
- *Från* Fokusering på standardens styrmedel *till* införande av relevanta åtgärder baserade på behoven och riskerna hos varje specifik organisation

I det följande diskuterar vi dessa två idéer.

9.5.1 *Från* IT-fokus *till* helhetssyn

Revisorerna upplever ofta att det finns ett obalanserat fokus och intresse för just IT-frågorna medan andra mjukare frågor som organisation, informationsklassning, och policies kommer i sista hand. Detta faktum har framkommit och kommenterats i tidigare frågor i undersökningen.

9.5.2 *Från* standardfokus *till* behovsfokus

Det verkar vara en missuppfattning att standardens krav skall gälla generellt för samtliga organisationer, eller i vart fall att de allra flesta av de styrmedel som föreslås där skall införas för att en lycksam certifiering skall vara möjlig. Så är inte fallet, vilket respondenterna påpekar. Det är till och med så att en organisation som blint inför alla de krav som anges i standarden utan att redogöra för behovet av detta kanske *inte kan* bli certifierat. Det kan finnas andra krav som ligger utanför standarden men som måste införas, liksom att det kan finnas kompenserande kontroller i form av styrmedel liknande de som beskrivits i standarden, som måste införas. Vidare förekommer det givetvis att vissa styrmedel, eller till och med hela grupper av styrmedel, i standarden inte är tillämpliga på grund av en organisations speciella risksituation. Ett enkelt exempel är att den organisation som inte har någon koppling till Internet naturligtvis inte behöver någon brandvägg för att skydda sig mot intrång via Internet. För organisationen handlar det alltså om att:

1. välja *ut* de styrmedel i standarden man *behöver*,
2. välja *bort* de styrmedel i standarden man *inte* behöver
3. *lägga till* andra styrmedel som inte återfinns i standarden men som krävs för en adekvat informationssäkerhet
4. *Valet av* både de valda och de bortvalda styrmedlen (enligt 1, 2 och 3) måste motiveras i ett så kallat ”uttalande om tillämplighet”. Dessutom måste utvecklingen och införandet av varje styrmedel avpassas till en för organisationen relevant nivå. Denna anpassning sker, vare sig man vill eller ej, i och med att styrmedlen konkretiseras i organisationen utvecklings- och införandefaserna.

Sammanfattningsvis; respondenterna ger uttryck för vikten av att fokusera mer på behovet av informationssäkerhet för en given organisation, än – vilket nu ofta är fallet – på det exakta innehållet i standardens exempel på styrmedel (även om dessa tjänar som en bra mall). Ett behovsanpassat LIS innebär inte bara att ledningssystemet kommer att bestå av andra kontroller än exakt de som återfinnes i standarden, utan även att varje styrmedel måste avpassas och införas så att de erbjuder en relevant nivå av säkerhet för organisationen. Om båda dessa utmaningar lyckas kan organisationen erhålla certifiering.

9.6 Övriga kommentarer

Fjärde och femte frågorna i enkäten till revisorerna löd:

> *Vilken är den viktigaste kunskapen Du har idag gällande LIS – och då specifikt certifiering, som Du skulle vilja berätta för andra som står i begrepp att skapa, införa och sedan certifiera ett LIS enligt SS627799?, samt*
>
> *Övrigt: Finns det något annat som Du vill ha sagt?*

Vi presenterar här avslutningsvis endast *några* av svaren på dessa uppsamlingsfrågor utan vidare analys eller diskussion av dessa:

9.6.1 Tips till den som står i begrepp att skapa, införa och certifiera ett LIS

> *"Gå utanför IT-sfären, samt tänk på att de dokumenterade kraven ska fungera i verkligheten."*
>
> *"Se till helheten och affärsnyttan."*
>
> *"Att inse att riskanalaysen som görs är en grund, grundval och utgångspunkt för att överhuvd taget kunna införa LIS"*
>
> *"Klargör tydligt syftet med införande av LIS och se systemet som ett hjälpmedel att nå den fastlagda säkerhetspolicyn / säkerhetsnivån"*
>
> *"Vikten av en väl genomförd, strukturerad och dokumenterad riskanalys."*
>
> *"Att i ett tidigt skede i projektarbetet förbereda åtgärder för upprättandet en kontinuitetsplan. Att ha en utvecklad metodik för uppbyggnad och införande av LIS."*

9.6.2 Övriga kommentarer

Ett utdrag av svaren:

> *"Standarden är otydlig i vissa avseenden är, men det krävs ännu mycken tolkningerfarenhet för att så småningom få en bra standard med rimlig efterlevnad."*
>
> *"Standarden, med skall-krav och best praxis kan verka förvirrande först. Många har inte tid att sätta in sig i standardens utformning utan vill ha ett snabbt svar och utgångspunkt att införa LIS. Det finns idag färdiga data-system som företagen kan köpa, som från dag 1 har färdiga kvalitetssystem. De behöver egentligen inte göra någon anpassning alls till sina egna processer. Denna utveckling är oroande. Om företagen köper denna gräddfil, kommer de att få stora*

problem vid certifieringen och fortlöpande problem vid uppföljande revisioner. Det är viktigt att stöta och blöta igenom alla problem inom företaget och se hur systemet kan växa fram och få växtkraft innan det kan utsättas för en oberoende tredje-parts granskning."

"Vi måste alla betona för företag/organisationer betydelsen av att ha och inte ha ett system för hantering av informationssäkerhetsfrågor, att inte underskatta tiden det tar att ta fram och implementera systemet samt betydelsen av en opartisk bedömning."

"Önskvärt att mer diskutera synen på medarbetare och deras kompetens, både som tillgång och hot. Standarden är här otydlig och tar egentligen inte hänsyn till serviceorganisationer och speciellt då kunskapsföretag"

10. APPENDIX C: ”KONSULTERNA OM INFÖRANDE OCH CERTIFIERING AV LIS”

10.1 Bakgrund

På uppdrag av SIS' LIS-projekt har Institutionen för Data- och Systemvetenskap vid Stockholm Universitet / KTH genomfört en kvalitativ enkätstudie syftande till att identifiera de erfarenheter och insikter deltagarna i projektets arbetsgrupp 3 erhållit beträffande införande och certifiering av ledningssystem för informationssäkerhet, LIS[1].

Genom att möjliggöra samarbete mellan informationssäkerhetskonsulter, certifieringsrevisorer, myndigheter (främst SWEDAC), och organisationer som söker certifiering, har arbetsgruppen sökt skapa och dokumentera unika erfarenheter. Syftet med denna rapport är att kommunicera dessa erfarenheter både inom och utom projekt LIS. Det torde finnas ett mycket stort intresse för detta, inte minst med tanke på att standarden nyligen blivit antagen av ISO som en internationellt erkänd standard, då med beteckningen ISO/IEC 17799:2000 (ISO 2000).

Informationssäkerhetskonsulternas och certifieringsrevisorernas erfarenheter och insikter studerades i två separata studier. *Denna rapport beskriver endast resultatet från studien av informationssäkerhetskonsulterna. Det finns en motsvarande rapport om revisorernas erfarenheter.*

I december 2000 nåddes en mycket viktig milstolpe för arbetsgruppen i och med att en av pilotorganisationerna blev tredjepartscertifierade enligt standarden (SIS 1999b). Därmed övergick arbetsgruppens fokus från att genomföra pilotcertifieringar till att dela med sig av alla de erfarenheter som skapats under de gångna åren. Denna studie och rapport är ett led i detta arbete.

10.2 Metod, demografi och reliabilitet

Undersökningen genomfördes som en skriftlig enkätundersökning med öppna frågor. Enkäten skickades ut till samtliga informationssäkerhetskonsulter som

[1] Originalrapportens titel är ”Informationssäkerhetskonsulternas perspektiv på införande och certifiering av LIS – en enkätundersökning”. Undersökning och rapport av Fredrik Björck som observatör i Projekt TK 099 ”Ledningssystem för Informationssäkerhet, LIS”, Arbetsgrupp 3 ”Pilotprojektet” (numera ”7799.nu”), SIS Standardisering i Sverige.

deltagit i "pilotprojektet" (AG3) inom standardiseringsgruppens (STG) projekt TK099 – Ledningssystem för informationssäkerhet. Totalt kontaktades arton respondenter med enkäten (*n=18*), och antalet svar efter *en* påminnelse slutade på tretton, vilket ger en svarsfrekvens på 72% (*(13/18)*100*).

Generalisering utifrån resultatet är inte nödvändig, då det inte finns någon bakomliggande population vi önskar dra slutsatser mot. Undersökningen skall ses som ett försök till kartläggning av unika erfarenheter hos de personer som deltagit i ovan nämnda pilotprojekt. Det är således fråga om en totalundersökning av den föreliggande populationen.

Samtliga respondenter har mycket gedigen erfarenhet av informationssäkerhetsarbete, och flera av dem var direkt involverade i en eller flera av de organisationer som sökt nå certifiering enligt 7799 (SIS 1999b) genom pilotprojektet. De tillfrågade lovades anonymitet i följebrevet.

Slutsatserna bygger på en strukturerad analys av det kvalitativa datamaterial svaren sammantaget utgör. Eftersom svaren samlats in elektroniskt från respondenterna minimeras de fel som annars ofta uppkommer vid inmatning på grund av överföring från ett media till ett annat (ex. vid avskrift av ljudupptagning för senare analys). Analysen av datamaterialet gick till så att varje svar (eller till och med *del* av ett svar) kodades med en kod som angav dess innehåll. Respondenternas olika svar på en given fråga (kontext) relaterades sedan till varandra med hjälp av koderna. Sakta växer då en modell (i det här fallet en visuell nätverksmodell) fram som visar likheter och skillnader i svar, samt som får oss att fokusera på det viktiga i svaren. Analysarbetet och den därpå följande induktiva processen (från enskilt svar via svarsmönster till slutsatser) underlättades av ett datoriserat metodstöd (ATLAS.ti), vilket gör det möjligt för andra att i efterhand kontrollera rimligheten i slutsatserna genom att undersöka vad – exakt vilka uttalanden/svar – respektive slutsats bygger på. En översiktsskiss som demonstrerar detta återfinns i slutet av rapporten.

Det har inte varit svårt att hitta gemensamma nämnare och mönster i svaren trots det låga antalet personer som deltagit i studien – tvärtom! Materialet visar på en närmast ofattbar samstämmighet, vilket ytterligare förvissar oss om att slutsatserna i föreliggande rapport är korrekta. Med korrekt skall förstås att; rapporten ger en riktig bild av hur de tillfrågade svenska informationssäkerhetskonsulterna ser på de undersökta aspekterna beträffande införande och certifiering av ledningssystem för informationssäkerhet enligt 7799 (SIS 1999b).

10.3 Framgångsfaktorer för införande

Den första frågan i enkäten till informationssäkerhetskonsulterna löd:

> *Vad anser Du vara de viktigaste faktorerna för ett framgångsrikt införande av ett ledningssystem för informationssäkerhet, LIS? (motivera gärna svar)*

Till skillnad från certifieringsrevisorerna (vilka fokuserade på *faktorer*), så fokuserade konsulterna mer på vilka *egenskaper/kunskaper* det enskilda projektet bör ha för att lyckas. Att arbetet med att skapa, införa och certifiera ett LIS bäst sker i projektform verkar därmed också vara en allmän mening bland konsulterna.

Analysen gick till så att varje uttalande, 37 stycken, kodades i två steg – först helt ostrukturerat och utan fördefinierade kategorier. Resultatet blev följande 23 kategorier av uttalanden:

- ability to put policy into practice
- accurate analysis of preceding security situation
- active employee participation
- active project members
- appropriate project organization
- backing from top management
- balanced policy grounded in reality
- clear aim from top management
- customer organization participation
- documented business processes
- feasible implementation method
- identifiable business benefits
- implementation know-how for project leader
- insight and knowledge about security
- integration with existing management systems
- monetary resources
- project ability to influence IT development
- realistic cost estimation
- realistic time plans
- regular communication with stakeholders

- top management awareness
- top management involvement
- understanding the need for security

En systematisk analys av kategorierna ovan resulterade i att de grupperades i – ansågs tillhöra – sex mer abstrakta kategorier, nämligen:

- Projektadministrativ förmåga
- Kommenderande förmåga
- Finansiell förmåga
- Analytisk förmåga
- Kommunikativ förmåga
- Exekutiv förmåga

För en helhetsbild av hur de olika kategorierna hör ihop med dessa sex övergripande kategorier – se nätverksdiagrammet i slutet av denna rapport.

Den följande presentationen av undersökningsresultatet för denna fråga utgår från de sex kategorierna.

10.3.1 Projektadministrativ förmåga (project management capability)

Projekthanteringskompetens - eller projektets förmåga att administrera och organisera sig självt i strävan mot målet (infört/certifierat LIS) - ansågs som en av de viktigaste faktorerna för ett framgångsrikt införande av LIS. Följande citat talar för sig själva:

> *”... realistiska tidsramar...”*
>
> *”... realistisk uppfattning om vad som krävs i form av tid...”*
>
> *”En aktiv arbetsgrupp...”*
>
> *”När ledningen väl beslutat om införande är det helt avgörande hur det projekt som skall införa LIS bemannas, organiseras, ges uppgifter, tilldelas resurser och genomför införandet.”*

Den projektadministrativa förmågan innefattar bland annat, vilket framgår av citaten, att projektets organisatoriska struktur är avpassad för dess uppgift, att det är rätt bemannat för uppgiften, att projektets medlemmar är - och ges möjlighet att vara – aktiva, samt att projektplaneringen tidsmässigt är realistisk.

10.3.2 Finansiell förmåga (financial capability)

En annan viktig framgångsfaktor som identifierades är att projektet som skall införa LIS i organisationen är har finansiell förmåga. De olika respondenterna utrycker sig så här:

> *" Klar målättning från företagsledningen, pengar,..."*
>
> *"Realistisk uppfattning om vad som krävs i form av tid och kostnader m m"*
>
> *"...väl tilltagna resurser..."*

Sammantaget är det främst två olika aspekter rörande just finansieringen av själva arbetet med att skapa och införa ett LIS som tas upp:

- att finansiella medel har avsatts för projektet, och
- att det finns en realistisk bild av hur omfattande finansiella resurser projeket totalt kommer att förbruka.

10.3.3 Exekutiv förmåga (executive capability)

Projektets förmåga att *omsätta dokument/idéer/regler i praktik* betonas av flera av de tillfrågade som en viktig framgångsfaktor. Förutsättningarna för denna exekutiva förmåga skapas med hjälp av flera andra kompetenser och förmågor:

- att projektledaren har erfarenhet från tidigare implementeringar av LIS,
- att man har en passande implementeringsmetod, eller i vart fall en idé om hur införandet skall gå till,
- att man har förmågan att att omsätta det som står i informationssäkerhetspolicy och regelverk till praktik, och
- att man har möjlighet att påverka IT-drift och –utveckling inom organisationen (för att på så sätt införa informationssäkerhet den vägen)

Några av de tillfrågade uttrycker sig så här:

> *"... Att kunna fullfölja - från policy till parameter. Många jobb stannar på policynivån, där de ju inte gör någon nytta. Policyn och standarden måste få effekt i det praktiska arbetet, och det är inte lätt. Tar antagligen år."*
>
> *"... framkomlig metod..."*
>
> *"En aktiv arbetsgrupp som har... inflytande på IT-utveckling"*

Projektets exekutiva förmåga är den som skall ta ledningssystemet från att vara ett dokument till att vara en beskrivning av en del av en verkligt fungerande verksamhet. I praktiken handlar det ofta om att man måste utbilda stora grupper medarbetare i organisationen för att åstadkomma förändring av beteenden så att det beskrivna ledningssystemet verkligen efterlevs.

10.3.4 Kommenderande förmåga (commanding capability)

Denna förmåga är direkt relaterad till den grad av uppbackning från organisationens ledning projektet erhåller. Uppbackning från ledningen beror i sin tur på ett antal faktorer såsom identifierbara affärsmässiga fördelar och ledningens förståelse rörande informationssäkerhetssituationen.

> *”Klar målättning från företagsledningen...”*
>
> *”Ledningens vilja och stöd... en organisation där det finns god förståelse för behov av säkerhet”*
>
> *”Högsta ledningens förståelse och engagemang”*
>
> *”Ledningen aktiva stöd då”*
>
> *” Ledningens stöd vilket förutsätter affärsmässiga fördelar med att införa det”*

Utan den kommenderande förmågan – innefattande rätten att i någon mån, å ledningens vägnar, ”ge order” till olika delar av organisationen - faller projektet platt.

10.3.5 Analytisk förmåga (analytic capability)

Några av delsvaren fokuserar på sådant som skapar förutsättningar för, och behovet av, en analytisk förmåga:

> *”Med erfarenhet från införande av andra ledningssystem är det oerhört viktigt att ha bra underbyggd nulägesanalys så att man kommer rätt från början.”*
>
> *”Det gäller även här och viktigast är förberedande grundarbete och faktaunderlag till informationssäkerhetspolicyn, m.a.o. se till att ha en verklighetsförankrad policy och med rätt omfattning”*
>
> *”... att verksamheten är processbeskriven eller motsvarande.”*
>
> *”... att LIS är en del av befintlig verksamhetsstyrning...”*

Det är den analytiska förmågan som skall hjälpa till att fånga upp den nuvarande (ursprungliga) situationen, och se vad som bör göras år den. Även integration med redan existerande regelverk, exempelvis ledningssystem för kvalitet och miljö, kräver analystisk förmåga om integrationen skall bli fruktbar.

10.3.6 Kommunikativ förmåga (communicative capability)

Den sista framgångsfaktorn som fångades upp i enkäten var just vikten av att kunna kommunicera med omgivningen på olika sätt. Detta skapar förutsättningar för aktivt deltagande från medarbetare i organisationen:

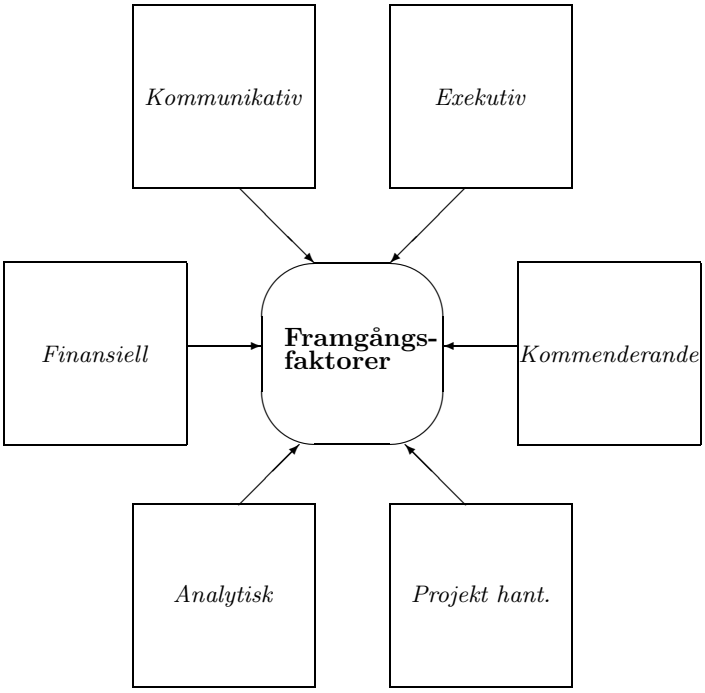


Fig. 10.1: *Framgångsfaktorer för lyckat införande och certifiering av ledningssystem för informationssäkerhet enligt SIS (1999b), ur informationssäkerhetskonsulternas perspektiv.*

> *"Förståelse, vilja och engagemang från den verksamhet i vilken LIS skall införas"*
>
> *"... att ständigt kommunicera och stämma av de olika delstegen"*
>
> *"Den egna personalen måste medverka aktivt"*
>
> *"Delaktighet från kunden"*

Citaten ovan nämner främst sådant som den kommunikativa förmågan möjliggör. Det spelar ingen roll hur bra projektet är i övrigt om det saknar förmågan att kommunicera sitt budskap till omvärlden – organisationen. Den kommunikativa förmågan kommer till användning i alla faser i projektarbetet.

10.3.7 Sammanfattning

Genom analys av den kvalitativa enkätundersökningens svar från informationssäkerhetskonsulterna inom projektet LIS, identifierades sex stycken framgångsfaktorer med avseende på framgångsrikt införande av ett ledningssystem för informationssäkerhet. Figuren ger en sammanfattande bild av dessa (se figur 10.1).

10.4 Metoder och metodverktyg i 7799-projekt

Den andra frågan i enkäten till konsulterna löd:

> *Har Du i samband med 7799-projekt tagit hjälp av någon metod eller någon typ av metodverktyg, exempelvis för dokumenthantering, inventering av tillgångar, riskanalys, gap-analys, projektstyrning, eller annat? (Om ja, ange gärna vilka metoder och hur Du tyckte att det fungerade)*

50% av de som besvarade frågan (*n=12*) har använt sig av en eller flera namngivna metoder eller metodverktyg för någon del av arbetet. Här följer en sammanställning av resultatet i tabellform (figur 10.2).

Metod / -verktyg	*Källa*
Riskanalys	
CRAMM	www.ccta.gov.uk
RA Software Tool	www.aexis.de
SBA Analys	www.dfs.se/sba
Nulägesanalys	
Bull Nulägesanalys	www.bull.se
Proteus	www.bsi-global.com
Projektstyrning	
PSM Projektstyrningsmodell	www.pejl.com
Assett management	
Comsecnordic ISMS 7799^{TM}	www.comsecnordic.se
Dokumenthantering	
BS5750:part 1:1979	www.bsi.org.uk
Doc Control	www.dokumentum.com
ITIL	www.itil.co.uk

Fig. 10.2: *Metoder och metodverktyg*

Ingen utav metoderna eller verktygen nämndes mer än en gång, vilket kan peka på att det ej ännu finns någon allmänt accepterad och vedertagen metod för konsulterna. De som inte har använt en namngiven metod har givetvis gått tillväga på något annat sätt – dvs använt en egen metod. SBA Check (www.dfs.se/sba - demo finns nedladdning), det av den Svenska Dataföreningen utvecklade svenska metodstödet för gapanalys mot bland annat 7799 nämndes inte av någon av konsulterna. Då SBA Check har runt 300 användare i Sverige då detta skrives så får man dra slutsatsen att användningen sker främst i andra sammanhang än i de undersökta certifieringsprojekten.

10.5 Fokus och tyngdpunkter i LIS-projekt

Den tredje frågan i enkäten till konsulterna löd:

> *Tycker Du att det (i det 7799-projekt Du tänker på eller generellt) funnits en bra balans vad avser fokus på datateknik-organisation, verklighetdokument, produktivitet-säkerhet (eller andra dimensioner)? Finns det delar som överfokuserats eller aspekter som fokuserats för lite? (förklara gärna svar)*

Ett utdrag av svaren:

> *"Det finns områden som inte tas upp som är mycket väsentliga för en organisation. Projektrutiner; hur och vilka faser skall beaktas i fråga om Informationssäkerhet då vi talar om projekt. Utan guidelines kan exempelvis en designer av hård/mjukvara fullkomligt demolera ett projekt genom att 'gjuta fel grund' och skapa en helt omöjlig situation för de som skal. Implementera säkerheten."*
>
> *"Ja, bra balans."*
>
> *"Egentligen inte (någon bristande balans) , men kanske vore ett bättre tydliggörande av ledningens ANSVAR som naglar fast den som chansar eller helt enkelt ger [tusan] i om olyckan drabbar företaget - vilket erfarenhetsmässigt är mycket vanligt. Kanske en juridisk fråga?"*
>
> *"Eftersom jag själv styr detta är jag nöjd med balansen så långt. En ev certifiering kan naturligtvis tvinga oss till en annan fokusering som man inte är helt nöjd med."*
>
> *"...jag tror att många kastar sig in i 7799-projekt utan att ha klart för sig vilken roll och betydelse IT har för verksamheten och hur IT är kopplat till affärsmål, strategi mm. Rätt svårt att prata säkerhet när vi inte riktigt vet vad som ska säkras!"*
>
> *"Begreppen LIS Informationssäkerhetpolicy - säkerhetpolicy har varit något frustrerande att definiera t.ex en policy för datakommunikation som är gränsen mellan olika företags policys man vill begränsa det till den digitala överföringen men taga med legala aspekter som att det skall vara lagligt osv. Detta kanske är hämmande att man inte har kunskap om ISO 9000 utan fokuserar på IT-system."*
>
> *"Ja, det finns en mycket bra grund att stå på för att visa att säkerhet inte 'bara' är en teknisk företelse, utan det är baserat på och är applicerbart just runt organisation och informationsflöde."*
>
> *"Det beror på hur kunden ser ut."*
>
> *"Nej! Många verksamheter fokuserar alldeles för mycket på tekniken. Förklaringarna kan var många. Min erfarenhet är att verksamhetscheferna har för lite kunskap om tekniken, vilket jag tror är på gång att ändras-det blir nog mer vanligt att f.d IT-chefer tar steget till att bli vd, och alltför gärna låter teknikerna få fritt spelrum. Vilken*

> *tekniker tycker om att dokumentera och sätta upp regler för sin verksamhet? Min uppfattning är också att det inte sällan klarlagts vilken nytta för verksamheten som IT-stödet skall utgöra."*
>
> *"Det finns ett för stort fokus på själva certifieringen."*

Analys av svaren ger vid handen att det främst är två skiften i fokus som önskas, sett ur konsulternas synvinkel:

- *Från* IT-fokusering *till* en helhetssyn på säker informationshantering, och
- *Från* Fokusering på standardens styrmedel *till* införande av relevanta åtgärder baserade på behoven och riskerna hos varje specifik organisation

Enkätundersökningen av certifieringsrevisorerna, vilken hade med exakt denna fråga, resulterade i liknande slutsatser (se gärna rapporten "*Certifieringsrevisorernas perspektiv på införande och certifiering av LIS – en enkätundersökning",* vilket är ett systemdokument till föreliggande skrift)

10.6 Övriga kommentarer

Fjärde och femte frågorna i enkäten till konsulterna löd:

> *Vilken är den viktigaste kunskapen Du har idag gällande LIS, som Du skulle vilja berätta för andra som står i begrepp att skapa, införa och certifiera ett LIS enligt SS627799?*

och

> *Övrigt: Finns det något annat som Du vill ha sagt?*

Vi presenterar här avslutningsvis endast *några* av svaren på dessa uppsamlingsfrågor utan vidare analys eller diskussion av dessa:

10.6.1 Tips till den som står i begrepp att skapa, införa och certifiera ett LIS

> *"Att man måste använda Standarden som ett ramverk där det krävs att man kompletterar denna med olika typer av del policys/ riktlinjer/ guidelines Och att man måste redan på ett tidigt stadium planera för att automatisera processerna samt uppföljning av dessa. Att inputen till regelverket kommer från människor som är verksamma inom respektive område. Tidigt även börja med utbildning av de olika grupperna som kommer att beröras"*
>
> *"Fördelarna med att ha ett genomtänkt och fungerande ledningssystem."*
>
> *"Att det är riskanalysen som avgör urvalet och nivån."*
>
> *"Hur oerhört överlägsen en STANDARD inom det här området är jämfört med alla guldgrävande tyckande konsulter som var och en har sin egen ide om hur säkerhetsproblemen skall angripas (vilket även jag har). Faktum är att absolut inget har skett ifråga om infosäkledning från det jag sysslade med detta på datainspektionen i 70-talets mitt och till 1995 när 7799 kom till."*
>
> *"Kanske att en grundbult är att identifiera och värdera/klassificera sina tillgångar (information, datorer, lokaler, försörjningsutrustning mm) så man vet vad som är skyddsvärt."*
>
> *"Låt inte 7799 överskugga allt annat. Bygg ett verksamhetssystem som passar ER, om det fungerar så bör rimligen 7799/ 9001/ 14001/ 17025/ USK m fl.... falla på plats av sig själv"*
>
> *"Aktivt deltagande"*
>
> *"Att det finns enormt många godbitar att hämta även ifall man inte är helt mogen att ta ett helhetsgrepp för ett införande, utan att man kan välja och vraka bland de delar som är prioriterade för stunden och man har vetskapen att dessa delar kommer att passa in även i*

ett nästa steg. Att det skapas ett enhetligt vokabulär inom organisationer och även utanför dem är en förutsättning då fler och fler vill t.ex. benchmark'a sig. Certifieringen skapar en förståelse för hur stort området är och hur man kan angripa ett eventuellt införande."

"Min erfarenhet från att arbeta i organisationer stora som små, att hantera relationer och andra verksamhetsrelaterade problem. Säkerhet är besvärligt för de flesta och det är väldigt viktigt att få en balanserad säkerhets anpassad just till aktuell verksamhet. Ibland är det vanligt att det blir 'för säkert'. En vanlig fråga bland yngre kollegor är eftergrågan av verktyg för att mäta vilken nytta som erhålls vid en viss vidtagen åtgärd. Min erfarenhet gör att jag har någotsånär lätt att utan verktyg uppskatta effekten av säkerhetshöjande åtgärder."

"Var helt på det klara med varför ett LIS införs och varför det är viktigt att certfiera detta LIS. Finns det inte ett solklart mål samt att frågorna är besvarade och accepterade så är mitt råd att 'skynda långsamt'."

10.6.2 Övriga kommentarer

"En sak som verkar ha stor betydelse för hur väl man lyckas är kvaliteten på den grunddokumentation som finns i företaget när processen startas. Detta har inte betonats tillräckligt."

"Man skall vara ödmjuk inför en sådan här uppgift. Den är omfattande. Jag anser att man när det gäller risk/konsekvensanalyser trampar in på ledningens område. Vi bör hålla oss mer specifikt till informationssäkerhet med IT-inriktning(Diskussionen har tidigare varit uppe!)."

"Kunder börjar nu efterfråga att leverantörer efterlever SS 62 77 99-standarden vilket kommer att vara påskyndande för införandet eftersom det då påverkar affärsmöjligheterna. Detta är betydligt mer drivande än om säkerhetsorganisationen föreslår ett införande, även om detta är välgrundat."

"Jag anser väl att standarden är skapad endast med tanke på stora företag och myndigheters verksamhet, där det finns stora resurser att investera i åtgärder som krävs för att uppfylla standardens krav. Med resurser inkluderar jag att det oftast finns en speciell organisation som bara arbetar med detta. För en mindre verksamhet skulle jag önska en omarbetning av standarden som på ett enklare sätt kunde plocka fram de relevanta kraven. Eller ett tillägg till standarden som guidar ett mindre företag, säg mindre än 50 anställda."

"Det skulle finnas ett antal förslag till Informationssäkerhetspolicy för olika branscher så att dessa skulle kunna vara det som förankras som modell först sedan modifiera beroende på HOT-bild och att arbetet läggs mer på riktlinjer."

"En organisation, ett företag eller vilken verksamhet som helst har mycket nytta av att införa ett ledningssystem. Det måste dock vara väl avvägt till just aktuell verksamhet."

11. APPENDIX D: HOW THIS RESEARCH CONTRIBUTED TO THE SOFTWARE TOOL SBA CHECK

Early ideas for the graphical user interface for a revised version of SBA Check. This version is dated March 16 1999. This non-functioning design study was created using Borland Delphi – a rapid application development environment for Windows.

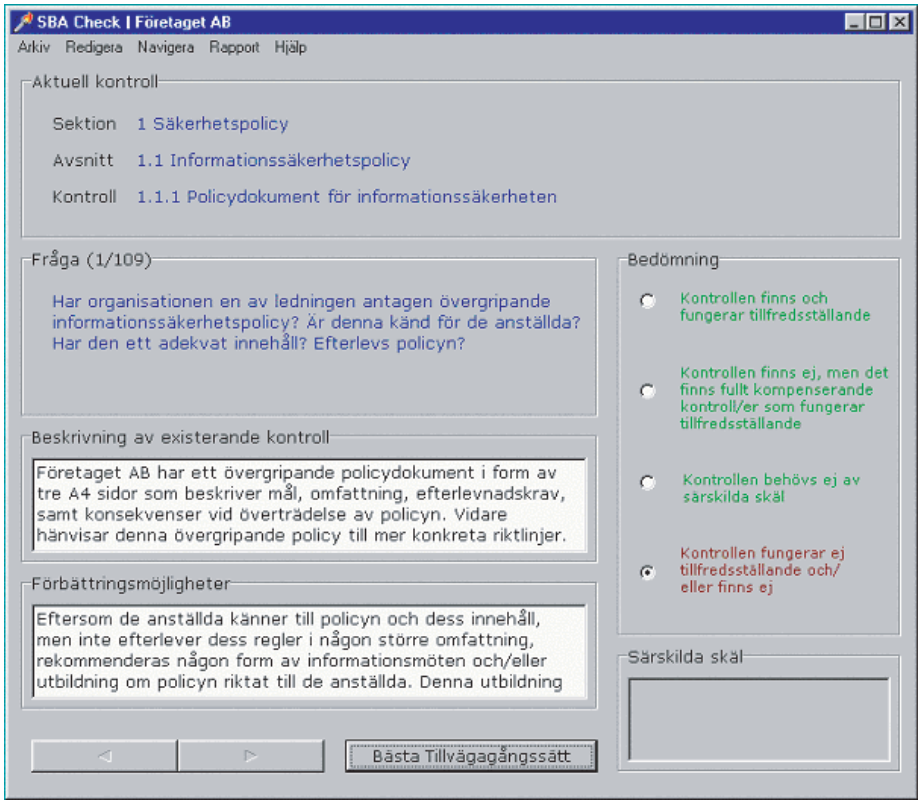


Fig. 11.1: *Early design study of SBA Check*

This version, from May 26 1999, is a primitive prototype. It was created in Microsoft Visual Basic, using Crystal Reports as its report generator component. This is the version that was included in the requirements specification, as a point of departure for the graphical user interface design. The 13-page requirements specification document was delivered from the research project to the Swedish Information Processing Society in June 7 1999.

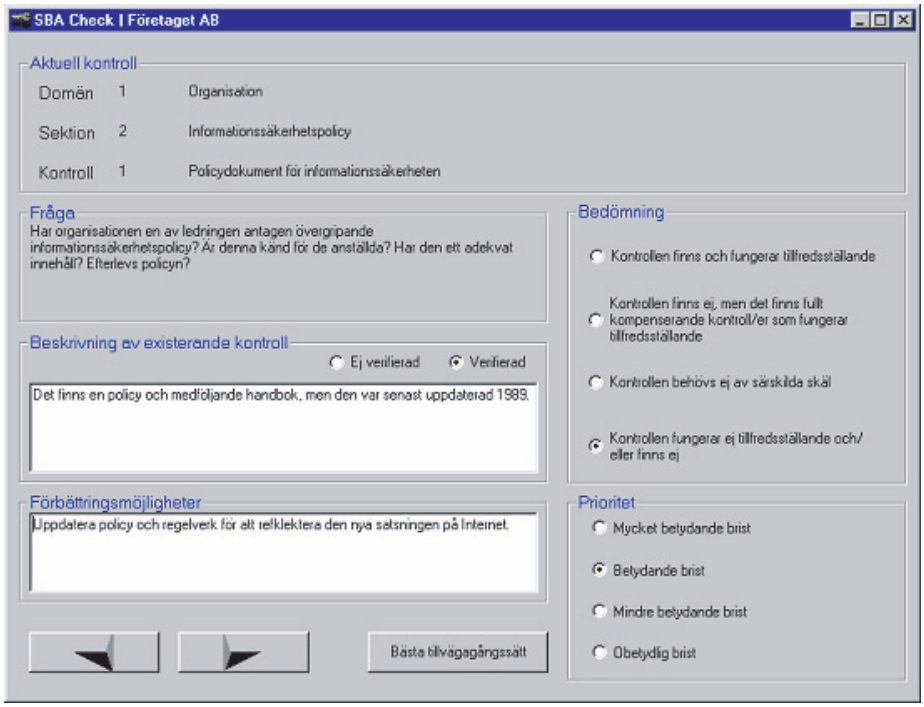


Fig. 11.2: *Primitive prototype of SBA Check*

This screenshot, from August 27 2001, is from the current version of SBA Check (4.x). It was developed by the programmers at Eyetee AB in Microsoft Visual Basic, using Crystal Reports as its report generator component. As can be seen from the pictures, most of the core evaluation principles behind the tool, originated as a part of this research undertaking, are left unchanged through the years.

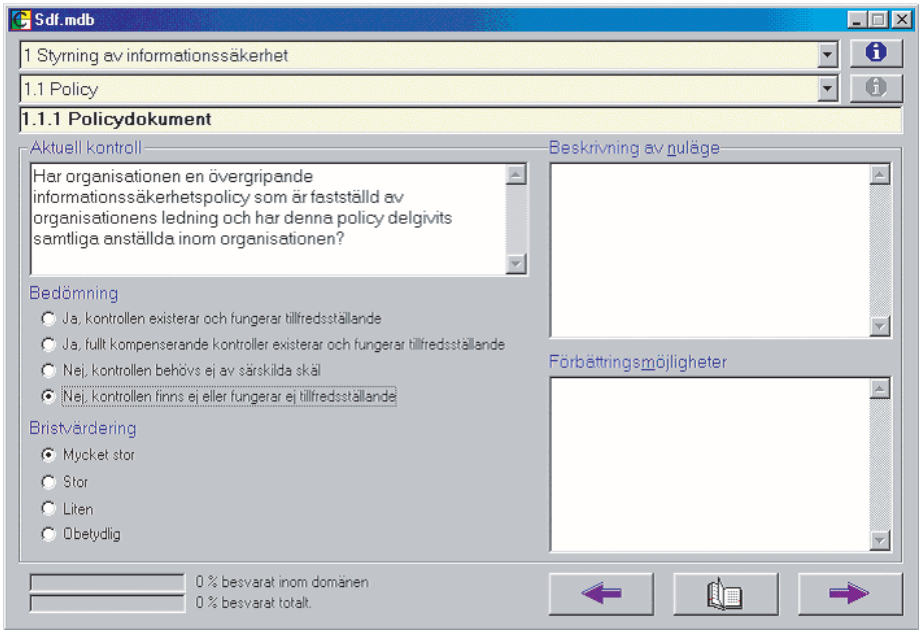


Fig. 11.3: *Current version of SBA Check (4.x)*

Fredrik Björck

- Security Scandinavian Style

Home | Projects | Publications

Fredrik Björck (www.bjorck.com)
Department of Computer and Systems Sciences
Stockholm University / Royal Institute of Technology
Forum 100, SE-16440 Kista, Stockholm, Sweden
Tel. +46 8.674.7498, Fax +46 8.703.9025
Email bjorck@dsv.su.se

(7799.nu visitors click here)

Björck is a Ph.D. candidate and lecturer at the Department of Computer and Systems Sciences, Stockholm University / Royal Institute of Technology. His research is focusing on certain aspects of information security management in organizations. He has served as vice president of ISACA (Information Systems Audit and Control Association) Sweden Chapter, is a member of the Swedish Information Processing Society and a Certified Information Systems Auditor (CISA). Björck is an information security consultant, currently on leave, at Ernst & Young, one of the world's leading professional services organizations. Björck holds degrees from the Växjö University (B.Sc. Business Studies and Economics, with studies in Japan at Ritsumeikan and in USA at George Mason University), and the London School of Economics (M.Sc. Information Systems Security). He is currently working towards his Ph.D. (Information Security) at the Stockholm University / Royal Institute of Technology.

Fredrik Björck and a team of information security experts have created SBA Check, an information security assessment methodology and software tool (in line with the ISO/IEC 17799 standard), which is marketed by the Swedish Information Processing Society.