School of Economics
and Commercial Law
GÖTEBORG UNIVERSITY

Department of Business Administration
Industrial and Financial Management
FE6000

INFORMATION RISK MANAGEMENT

- *A case study* of major Swedish banks concerning the concept of information risk management -

Kandidatuppsats/Bachelor Thesis

Authors:
Vilhelm Brag, 771012
Frida Wedefelt, 780225

Tutor:
Anders Rimstedt

Business Administration/
Industrial and Financial Management
Spring semester 2004

School of Economics and Commercial Law
GÖTEBORG UNIVERSITY

ABSTRACT

Given the information- and knowledge-intense characteristics of the modern world, there is no surprise that information risks and security is a growing concern among most companies. The managing of these risks is therefore increasing in significance. In this thesis we addressed issues concerning information risk management, which is about managing risks associated with disclosure, modification, unavailability or destruction of information. The research was conducted in order to clarify the perceptions along with the involvement and awareness of information risk management. Our investigation approach consisted of qualitative interviews, in the form of case studies, with risk managers at four major banks in Sweden. The work, which was carried out in cooperation with KPMG, resulted in a better understanding of how information risk management is structured and organised as well as which information risk areas are considered to be included in the concept of information risk management. The main conclusions drawn from our research firstly, emphasised the importance of reducing information risk by securing the availability, confidentiality, integrity and traceability of the information, and secondly, showed great awareness and commitment for these issues among top management as well as among employees within the organisations.

Key words:
Operational risk, Information risk, Risk management, Information Security, Bank.

School of Economics and Commercial Law
GÖTEBORG UNIVERSITY

ACKNOWLEDGEMENTS

We would like to express our gratitude to a number of people, who have helped us along the way, and made the accomplishment of this thesis possible. First of all, we would like to thank Anders Rimstedt, our tutor at the Department of Industrial and Financial Management, for his encouragement, support, and feedback to our work. We would also like to express our appreciation to our tutor at KPMG, Tobias Carlén, for his interesting thoughts, suggestions, and eminent supervision. Lastly, we would like to thank the interview respondents at SEB, FöreningsSparbanken, Danske Bank and Nordea for their valuable contributions to the thesis.

Gothenburg, 14th of June 2004

Vilhelm Brag & Frida Wedefelt

School of Economics and Commercial Law
GÖTEBORG UNIVERSITY

TABLE OF CONTENTS

School of Economics and Commercial Law
GÖTEBORG UNIVERSITY

TABLE OF FIGURES

1 INTRODUCTION

In this first chapter we will briefly present the background of the research area to provide the reader with a fundamental understanding about the topic of risk management. We will also present the problem area as well as our problem definitions in order to explain the subject that we are going to study.

1.1 BACKGROUND

1.1.1 CHANGES MEAN RISK

The world is constantly changing. Changes are unpredictable and their effects most often hidden. Changes rarely come with undesired consequences for humans as well as for organisations. Change means risk. The word risk captures both the effects of change and our inability to predict that change (Marshall, 2001). Risk can broadly be defined as "the potential for events or ongoing trends to cause future losses of fluctuations in future income" (Marshall, 2001 page 24). As a normal part of doing business all companies face risk. These risks arise from external forces that are beyond a company's immediate control and from a number of internal forces that can and need to be managed (Bowling & Fredrick, 2003). As our knowledge and understanding of the impacts and causes of the changes in the world around us increase, the risk that we are faced with decrease. But no knowledge can remove all risk. Some risks are inherent to business and acceptance of these core risks is an important introduction to managing risk. It is essential to bear in mind that risk management does not mean total risk elimination (Marshall, 2001).

1.1.2 DIFFERENT KINDS OF RISK

The risk faced by most companies can typically be broken down into *market*, *credit*, *strategic* and *operational* risks. Market risks are those fluctuations in net income or portfolio value resulting from changes in particular market risk factors. Credit risk are fluctuations in net income or net assets values that result from the default of a counterpart, supplier or borrower. Strategic risks are those long-term environmental changes that can affect how business adds value to its stakeholders (Marshall, 2001). Operational risk is by far the most extensive risk category and therefore demands the most general approach (Marshall, 2001; Hussain, 2000). Thus operational risks consist of threats coming from factors such as people, processes and internal systems, as well as external events. Unlike market and credit risk, the data concerning operational risk is

difficult to grasp. A lot of the data is instead qualitative and subjective while credit risk and market risk data is more quantitative related (Marshall & Heffes, 2003).

1.1.3 RISK IN THE REAL WORLD

Corporations have always taken risk management very seriously; in fact, several surveys claim that executives have ranked risk management as one of their most important objectives. The literature on why firms manage risk at all is usually traced back to 1980'ies and since then the use of risk management strategies have increased dramatically (Cassidy, et al, 1990). Nowadays, risk management is the paramount topic amongst board of directors and other persons within the management of companies and most large and medium-sized companies carry out risk management to some degree (Waring & Glendon, 1998).

1.2 PROBLEM AREA

In our thesis we are going to focus on the information risks, which have increased due to the development in information technology. Technology and techniques have undergone an immense change over the past 40 years, to culminate over the past ten years when the development has been extraordinary, and the implications for operations profound (Marshall, 2001). Information technology includes risks on different levels and since it is constantly evolving it does not provide a complete coverage of all those risks. Further, the information systems and transfers are not totally reliable. Errors can easily appear in unstable environments and any missing information is a source of risk. There are many potential causes for deficiencies. Broadly, information might be improperly disclosed, modified in an inappropriate way or destroyed or lost (Blakley et al, 2001). Any deficiency in information risk management potentially generates losses of an unknown magnitude. Given the information- and knowledge-intense characteristics of the modern world, there is no surprise that information risks and security is a growing concern among most companies and the managing of these risks are therefore increasing in significance (Bessis, 1998).

Every organisation is more or less exposed to information risk such as leakage or modification of information. Financial services, such as banks, which deal with risk management on an everyday basis, appear to be an industry that has a vital interest in information risk management. Nevertheless, global survey finds that large banks and other financial institutions are suffering multimillion-dollar losses as a result of poor risk management. For example, a survey by Risk Waters Group and SAS found that one of five financial companies still does not have an information risk management program, yet 90% of these companies lose more than $ 10 million

a year because of poor risk control practices. The losses could be caused by transaction error or fraud, system failures and resulting downtime as well as by inefficiencies or mismatching of transactions. (Marshall & Heffes, 2003; Computergram Weekly, 2003)

The matter concerning protecting the correct information with the right solutions, both technically and administrative, is a reoccurring topic within the area of information risk management. According to research material and studies that we have acquired from KPMG, we have found that despite accepted rules and policies there are only a few companies that follow them. We therefore believe it is interesting to study the information risk, in terms of how it is perceived, as well as what kind of efforts are undertaken to manage them.

Further, according to our tutor at KPMG and resent debate articles (Rathmell, 2002) the main part of the work and the solutions that are implemented in the frame of information risk management, are mainly focused on technical aspects and neither closely associated to the main requirements nor the fundamental risk policies of the firm. Accordingly, it is rather common that IT managers and IT divisions have full responsibility for the information risk management of the organisation. As a result the risk management might be reduced to cover only technical security solutions within the IT maintenance area. Narrowing the risk issues like this might cause severe damage such as large losses, both in the form of information and capital. Following this reasoning it becomes relevant to study what the situation looks like in the actual business reality. It is interesting to study whether technical aspects are the centres of attention concerning information risk management. It is also relevant to study management's awareness and involvement in issues concerning information risk management.

1.3 PROBLEM DEFINITION

Based on the discussion in Problem Area, we have formulated a main question. The main question is broken down into six different sub questions in order to make our research more specific and precise. The purpose is also to make it easier for the reader to follow the main thread starting from the six sub questions, continuing throughout the theory, findings and analysis and at last ending up in the conclusions.

The problem definition of the thesis is:

Investigate the concept of information risk management and how it is perceived within major banks in Sweden.

To make the general problem definition more specific, we have chosen to divide it into sub questions, which follow below.

As mentioned above, risks faced by most companies are broken down into market, credit, strategic and operational risks. When studying literature concerning information risks it is not directly discussed in the context of any of the above four risk areas. Yet, since it seems naturally that information risks arise in the different operational flows within a business it might be likely that information risk management falls under the management of operational risks. We would like to straighten this out. In order to do that we will start of with the following question:

- *How is operational risk defined and what responsibility areas are included in operational risk management?*

Information risk management is a new area and it is difficult to find concrete theory about the matter. When trying to grasp the concept of information risk management, we are faced with ambiguous definitions and different characteristics of the risk area. Therefore, we would like to understand how information risk is perceived and what kind of risks areas that are put into the concept of information risk management. Is it technical risks such as system failure, or is it organisational risks such as failures in rules or policies, or is it any other kinds of risks. In addition, how is the work with these issues structured? This leads us to the following questions:

- *How is information risk defined?*
- *What responsibility areas are included in information risk management and how is the work structured?*

Further, it is interesting to study what concrete risks that threaten the information within the companies and what is done to diminish these risks. Is the lion's share of the work, solutions and capital invested in technical issues such as hardware and/or software or is a more holistic organisational approach used covering issues such as availability, integrity, authentication and confidentiality to protect the information. Accordingly, the next question at issue is:

- *What main risks constitute a threat to the information and how is the information secured?*

As said earlier, during the past decade society has moved towards an information- and knowledge environment. The value of firms has become more based on intangible assets rather than tangible assets. Banks are building their entire businesses on information flows and information technology. We believe it is interesting to investigate whether the comprehension about information risks and the origin of the risks has changed due to this evolvement and also what kind of risk development can be expected in the future. Thus the next question to investigate is:

- *What kinds of changes concerning information risk have been most legible during the last decade and what kind of changes are expected in the future?*

The top management decides upon how much risk the bank will bear in order to reduce the probability of a major corporate disaster and ensure the bank's success in the market place. To tie the knot we would therefore like to:

- *Investigate the extensiveness of top management's awareness and involvement regarding information risk management.*

1.4 PURPOSE

The purpose with this thesis is to investigate the concept of information risk management in order to define and clarify the perception and importance of the concept within major banks in Sweden. The aim is to understand the commitment and awareness of information risk management within the banks. This is done in two parts; first a study of the topic on a theoretical level is performed, in order to obtain a thorough knowledge of the subject. Thereafter hands-on knowledge is to be obtained by studying the context on a practical level when performing interviews out on the field.

1.5 DELIMITATIONS

The focus of the thesis will only be put on operational risk and information risk management; we will neither deal with market, credit nor strategic risks. Further, we are neither going to provide any new approaches nor any proposals on improvement within information risk management. Since the time horizon is rather short we will delimit the thesis to include a fundamental research within the area of information risk management. We will put our main focus on comprehension of the attitudes and the perceptions of the concept. Interesting research outside the frame of the thesis is discussed in the section called Further research.

1.6 DISPOSITION

The thesis can be divided into seven parts, which together provide a clearer picture over the structure of the thesis (See figure 1).

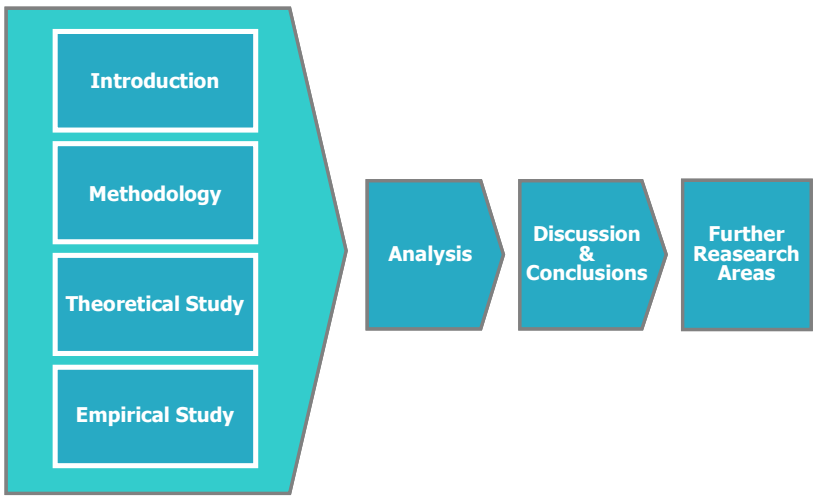

Figure 1 Disposition

Introduction

This chapter will give a background of the thesis project. Problem area, Problem definition, Purpose, Objectives, Delimitations, and Disposition are presented.

Methodology

In this part we will give an overall description of methodology and the applied methodology path in the thesis. The Course of Action of the thesis is also presented.

Theoretical Study

Here we deal with the theoretical aspects of our thesis work and fundamentals to our studies.

Empirical Study

The research study and the qualitative study are carried out and presented. We will also give a brief description of the chosen respondent i.e. the interviewed organisations.

Analysis

The findings from our studies are analysed in relation to the theory.

Discussion & Conclusion

We discuss our findings as well as relate them to our purpose and problem definition. Our main conclusions from the analysis and discussion are thereafter summarised.

Further Research Areas

Finally, we present some thoughts and reflections on further research and what aspects we find interesting to study closer.

2 METHODOLOGY

This chapter gives a brief description of theories related to the following methodological areas; philosophical perspectives of research design, different approaches to research design, and finally the course of action applied during the evolvement of this thesis. The overall purpose of the chapter is to explain the various aspects of methodology and to present our chosen methodological path.

2.1 PHILOSOPHICAL PERSPECTIVES

In order to conduct and evaluate a research it is important to know what underlying assumption that constitutes a valid research strategy and what research approach that is most appropriate. In the literature, classifications of underlying method traditions in empirical science are discussed (Wallén, 1996) and we have chosen to bring up the most common i.e. *positivism* and *hermeneutic*.

Positivists argue that human beings only have two sources of gaining knowledge: (1) what can be registered with human senses, and (2) what can be reasoned with human logic. The positivists claim that such non-empirically proved attitudes do not belong to the scientific sphere. The theory of positivism has also got an ideological side; everything not regarded as scientific knowledge cannot be regarded as knowledge at all and/or just as irrational knowledge. (Wallén, 1996) Hermeneutics can roughly be translated as the school of interpretation. The hermeneutic approach perceives the worlds as an individual, social and cultural construction and knowledge cannot be separated apart from the person (Backman, 1998; Alvesson & Sköldberg, 1994). The researcher should focus on process, interpretation and understanding. The perspective goes hand in hand with qualitative, inductive methods (Merriam, 1994).

2.1.1 APPLIED PHILOSOPHICAL STANDPOINT

Within the hermeneutic theory, comprehension is described as a circle or spiral. This circle contains of understanding, comprehension in relation to the overall picture, new understanding, and so forth (Alvesson & Sköldberg, 1994). Since we will be studying a rather complex and undefined concept we have chosen to base our study on the hermeneutic approach.

We will, when following the hermeneutic approach, gain pre-understanding of the subject through literature studies, which will be followed by a more thorough comprehension achieved through the interviews. By following the hermeneutic path we will firstly; during the interview phase get the opportunity to get given answers clarified and confirmed with the respondents,

insuring that we have understood them correctly. Secondly, by reflecting the theory in relation with the obtained interview result, we will accomplish a deeper understanding based on the interpretation of the material, which will act as a comprehensive base when formulating the conclusion.

In the sections below we will further present what kind of methods used within the frame of the hermeneutic perspective.

2.2 RESEARCH DESIGN

When it comes to describing research design, difference is made between the qualitative and the quantitative approach. Within social scientific areas the quantitative approach is most widely used, however, qualitative research is making progress and thereby becoming more and more common. This shift is much due to the fact that qualitative research is creating conditions to give a broader and richer description of concerned individual ideas (Alvesson & Deetz, 2000). Below, the concerned approaches will be further described.

2.2.1 THE QUANTITATIVE APPROACH

Quantitative methods are more formularised, structured and characterised by the researcher's control. The quantitative methods define the kind of relationships, which are of special interest on the basis of the problem definition and they are characterised by selectivity and distance from the interview object. This is absolutely necessary if formularised analysis and comparisons are going to be conducted. Statistical methods for measurement are important in the analysis of quantitative data since it based on those is possible to comment on the viewpoints and opinions of the respondents. It is also possible to obtain a cross section of the existing opinions. The method is however not suitable when trying to obtain information about social or environmental processes. New knowledge that evolves during the concrete realisation of the investigation must not result in changes in the planning or structure of the research. (Holme & Solvang, 1997)

2.2.2 THE QUALITATIVE APPROACH

Qualitative studies often aim to discover the character of a phenomenon, how it should be identified etc. The main difference between the quantitative approach and the qualitative approach is that in the latter the reality is not viewed as objective but subjective. The reality, in the qualitative approach, is an individual, social, cultural construction. It is more important to study the human perception of the reality rather than, as in the quantitative approach to study

and measure a given "reality". In the qualitative approach the reality is not separated from the individual as it is in the conventional approach. The qualitative approach emphasises conceptions, and the individual interpretation as knowledge source instead of focusing on empirical material. The qualitative approach has an impact on the research process. Overall the process becomes more dynamic and flexible in comparison to the quantitative research process. Furthermore, the activity of interpretation and analysis becomes more evident when the researcher chooses to adapt a qualitative approach. (Wallén, 1996; Holme & Solvang, 1997)

2.2.3 APPLIED RESEARCH DESIGN

Based on the presentation of the research designs above, we have come to the conclusion that the qualitative approach is best suited for our research and studies. Therefore we will present the qualitative research wheel a bit further in this section and then go through how we applied it for our study.

The starting point of the qualitative research wheel consists of the researcher's prejudices and pre-comprehensions. The pre-comprehensions is the same as the researcher's view of a certain phenomenon or occurrence, which he has gained through experiences, educations or other scientific work. Prejudices are also fundamental whenever a research is to be initiated. The prejudices are socially based, personal opinions concerning the phenomenon or occurrence that is to be examined. The qualitative research process is based on an analytical difference between the value based opinions and the opinions based on pure facts. These two aspects represent two hermeneutic circles, one cognitive and one normative circle (See figure 2). (Holme and Solvang, 1997)

Figure 2 The qualitative research wheel (Holme och Solvang, 1997)

The cognitive circle has its starting point in the pre-comprehension and the normative circle has its starting point in the socially based prejudices. There exists a reciprocal action between the cognitive and the normative elements as well as between the researcher and the research objects. The aim is always to obtain better knowledge! Through our education we have achieved a certain pre-comprehension concerning different types of risk management. We understand the fundamentals about how it is defined and what is included. Further, through in-depth studies of the subject we have gained a fundamental understanding about operational risk management as well as information risk management and based on that we have created our, so called, pre-theory. Thereafter, based on that pre-theory we will develop new perceptions and opinions, which we will try against the viewpoints of our interview objects. Due to experiences and perceptions, created by ourselves influenced by the world around, we are aware of our prejudices concerning these concepts. We understand the importance of keeping this in mind when meeting our interview objects, in order not to influence them with our own prejudices. We aim to critically try our perceptions against the perceptions of the interview objects. To be able to do this we have decided to carry out case studies, where the concept of information risk management is the case, which we will study in four different environments. The case study is explained below.

2.2.3.1 The Case Study

Yin (1994) defines *"A case study is an empirical inquiry that investigates a contemporary phenomenon within its real-life context when the boundaries between phenomenon and context are not clearly evident and in which multiple sources of evidence are used"* (Yin, 1994, p. 13). Within the scope of a case study, we will strive to discover and explore new conceptions as well as gain better understanding for the concept that is studied within the frame of the case study. Case studies are preferable when research is focused on "how" and "why" questions, which is exactly the issue in our study (Yin, 1994). According to Backman (1998) a case studies is appropriate when the objects at study are rather complex, e.g. when phenomenon, organisations or systems are to be elucidated, understood or described. Our research is going to be focused mainly on information risk management but also on operational risk management, which both are relatively ambiguous and indefinite concepts. Since the issues demand a lot of clarification and discussion we consider case studies to be a very good choice for the purpose of our study.

2.3 COURSE OF ACTION

In this section we will briefly present the course of action we have taken throughout the work of our thesis. Our course of action has been the following: 1) Choice of research area, 2) Literature studies, 3) Interviews, 4) Evaluation and analysis, 5) Conclusions. (See figure 3).

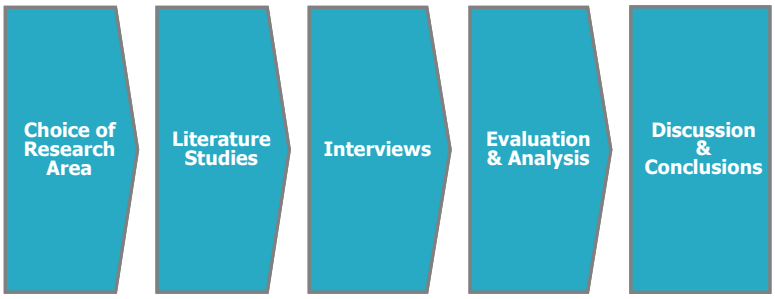

Figure 3 Our course of Action

2.3.1 CHOICE OF RESEARCH AREA

During courses within Industrial and financial management, which took place throughout the first half of this semester (Spring 2004), the topic of risk management especially interested us. Searching for an interesting thesis topic, we came in contact with the audit, tax and financial advisory firm called KPMG. The firm has a thesis program, which we applied for and was accepted to. KPMG was interested in cooperation with students who wanted to be involved in research and studies concerning information risk management. Since both of us have a Master of Science degree in Informatics from prior studies this area of research seemed existing and inspiring. In this sense we were able to combine our knowledge and experience from the information technology area with our new knowledge from the financial area. We were assigned a tutor, Tobias Carlén, who works as an information risk management specialist and therefore has comprehensive knowledge and experience within the area. In discussions with Tobias Carlén, we learnt that the understanding and handling of information risk has increased in importance due to the development of information technology. Yet, the understanding and handling is not well established. As said in the problem definition, the perception of the concept is rather ambiguous and the main part of the work and the solutions implemented are mainly focused on technology, which is not associated with the main requirements and the fundamental risk policies of the firm. In addition, the top management does not seem to be involved in the process of information risk management in the same way that they are in other risk issues. On the basis of the discussion

with Tobias Carlén about these potential problems we decided to focus our research on the concept of information risk management and its importance within organisations.

2.3.2 LITERATURE STUDIES

Yin (1994) advocate that literature studies are one of the most essential parts of the case studies since it brings clarity and understanding for the research area and the problem at issue. On the other hand, it could be negative if the researcher obtains preconceived notions about the research area depending on the work of other researches and laymen (Backman, 1998). In other words, it is essential to start the literature study with a neutral and open mind. To provide ourselves with a solid knowledge base to start off from, we began with a general literature review of the topic, studying areas such as operational risk management, information security and information risk management. Due to this general study we were able to delimit our research area and get more structured before we began with more in-depth literature studies, focusing more on operational risk management and information risk management. To be better prepared for the meetings and interviews with the research objects we found the in-depth literature studies to be very important and helpful. The literature study, which also could be defined as our secondary data gathering, took place during the whole research and writing process.

2.3.3 INTERVIEWS

Qualitative interviews are quite a demanding way of carrying out primary data gathering. Since our interviews were of qualitative nature, they were not formalised to a great extent, instead our intention was to go through our questions with the respondents, which in turn would result in further discussions concerning the subject. We were therefore not bound to strictly follow the questions in the guide one after another as long as we obtained answers to all the questions we wanted answered. The purpose of qualitative interviews was to increase the value of the information and obtain a deeper more thorough understanding of the concept. Therefore our selection of interview objects became fundamental and we had to base the selection on carefully formulated criteria.

In our discussions with our tutor at KPMG we decided that risk managers, at different banks in Sweden, would be interesting to meet for interviews. The basic idea was that they deal with different kind of risks everyday and would certainly have something to say about the matter. Also, the banks have lately built their businesses much on information and information technology. Further, as pointed out earlier, global survey found that large banks and other financial institutions are suffering large losses as a result of poor risk management and we

thought that interviewing risk managers at banks would provide us with an insight in the risk management issue. Since qualitative interviews are, as said earlier, an arduous form of information gathering, it set some demarcations for how many interviews we could carry out. We picked out the largest banks in Sweden and contacted them through e-mail and telephone. We received a positive answer from four of the selected banks. The fifth bank never returned to us and we decided to conduct four in-depth interviews with banks that did have interest in the research. The banks were: SEB, FöreningsSparbanken, Nordea and Danske Bank. They are all large and well-established banks in Sweden with lot of experience in risk management. At FöreningsSparbanken we got the opportunity to talk with both the operational and information risk managers. At SEB we met with an operational risk manager along with two information risk managers from the Merchant Banking of SEB. At Danske Bank we interviewed the Chief of Security and at Nordea we got the opportunity to interview the operational risk manager. Why the number of respondents varied from case to case is due to the fact that we wanted to cover a wide area of knowledge as possible. We did however not specify the number of respondents in advance.

The interviews took place 29 April 2004, in Gothenburg and 6 and 7 May 2004, in Stockholm. The reason for this approach was that we were not able to synchronise our schedules with the schedules of all the respondents and therefore we had to carry out two telephone interviews from the office of KPMG in Gothenburg. The interviews in Stockholm took place at respective interview object's bank office. We were both present at all three interview occasions to be able to divide the interview work in two parts or roles, one interviewer and the other taking notes. We documented the interviews with the help of a dictaphone, notes and our sharp memory.

There are several interview techniques that one could use, and we decided to use the type, which called *informant* and *respondent interview* on a *discussion basis*. Respondent interviews are interviews with persons who are directly involved in the area at study, and the informant interviews are interviews with persons that themselves are outside the area at study at study but indeed has a lot to say about it (Holme & Solvang, 1997). We believe that the interviews are a mix between these two. The bank managers are very much involved in the risk management, but at the same time they can be relatively objective and report the perceptions and awareness of all the employees concerning information risks management. After having conducted the study, we must say that we succeeded in the matter finding the respondents that could give us the all-embracing view that we looked for.

2.3.4 EVALUATION AND ANALYSIS

The part were we do our analyses should according to Backman (1998) have a certain structure or categorisation. According to Yin (1994) there does not exist a predetermined way of writing the analysis. It is rather up to the researcher and his way of looking at and evaluating the research material. In our findings chapter we structurally presented the interview results from the different organisations and in the analysis chapter we compared and evaluated the results in relation to the theory in order to draw parallels and comment back and forth on the findings. Thereby we follow the most common strategies for analysis, i.e. contemplating and reflecting the primary gathered material in relation to the theory. The aim is to in the end come up with new insights (Yin, 1994).

2.3.5 DISCUSSION & CONCLUSIONS

In this chapter we related the analysis to our purpose and problem definition. We draw conclusion based on our analysis and wrapped up what we believe are the most important findings of our research study.

2.4 EVALUATION OF THE THESIS

Validity and reliability are both important aspects in research studies. In this section we will present how we have increased the validity and reliability of our study. We will also bring up what factors might negatively have affected the validity and reliability of our research.

2.4.1 THE VALIDITY OF THE THESIS

According to Thurén (1996), validity refers to the degree, which a study accurately reflects or assesses the specific concept that the researcher is attempting to measure. Thus, validity is concerned with the study's success at measuring what the researchers set out to measure. It is however difficult, if not to say impossible, to guarantee that a research method is valid or not (Lekvall & Wahlbin, 1993). It will never be possible to measure the "true" value of any research method only subjective appraisals are possible. As mentioned above in the course of action, we prepared ourselves carefully by studying relevant literature within our problem at issue, in order to increase the validity of our research. By being well read prior to the interviews we hoped to improve the validity.

Before conducting the interviews we had a meeting with our tutor at KPMG, in order to obtain his feedback to our interview questions. By letting him, as a specialist within the area, review the

interview questions we believe the validity of the research increased. The validity also increased considering that we let the respondents take part of the interview questions a few days prior the actual interview. In that way we reduced the risk for misunderstanding of the question and the respondents were also able to prepare themselves for the interview. Since we conducted a qualitative study we also sought to ensure a high level of discussion within the specific topic area. By giving the respondents the opportunity to review the questions in advance, we were able to obtain rewarding interview material. In addition, by giving the respondents the opportunity to read through the interview results, in order to get their approval before moving on with the analysis, the validity of the research was further improved.

Finally, the validity of our study may have been negatively affected due to the selection of our interview objects. We can never be sure of having interviewed the right persons. On the other hand we know that the respondents fulfil the criteria set up for being part of the research, i.e. they are either head of operational risk, information risk or security at the respective banks. We were careful to ask them, before setting up a meeting, if they were able to answer our questions concerning operational risk management and information risk management.

2.4.2 THE RELIABILITY OF THE THESIS

Reliability is the extent to which an experiment, test, or any measuring procedure yields the same result on repeated trials. Without the agreement of independent observers' ability to replicate research procedures, or the ability to use research tools and procedures that yield consistent measurements, researchers would be unable to satisfactorily draw conclusions, formulate theories, or make claims about the generalisability of their research (Writing@CSU, 2004). Patel & Davidsson (1994) claim that if interviews are used as a method, the reliability is dependent on the interviewer's ability and technique in the context.

In order to improve the reliability we conducted test interviews, which strengthened our self-confidence for the interview situation. To further guarantee the reliability of the findings from the research it is important that the questions in point are understandable and unambiguous (Lekvall & Wahlbin, 1993). Reliability is according to Thurén (1996) equivalent to credibility, which implies that the conducted research is carried out correctly. To increase the reliability of our research we tried to make the questions easy to comprehend for the respondents. We were careful neither to use formulations of wording too obvious nor too leading. To make it easier for the respondents we also organised the questions into different subjects. The questions were mainly of general character, with the intention to initiate more in-depth discussions, where the

respondents would feel comfortable and relaxed to talk about his/her perception of the area at subject.

Further, another way of increasing the reliability of the research is to use a tape recorder or a dictaphone when conducting the interviews as well as when summarising the interview material. The approach results in increased creditability, since it is possible to go through the recorded material over and over again to ensure that the contents of the interviews have been understood correctly. (Patel & Davidsson, 1994). By using a dictaphone during all our interviews, the reliability of our research improved.

However, the reliability of our research might be dubious. To start with the reliability may at the same time have been negatively affected since the quality of the recording was not always the best. It has sometimes been difficult to hear and understand what the respondents are saying and as a result, complicated to print out correctly. Further, our respondents have somewhat different roles within their organisations, which could result in them focusing on different aspects. Also the selection of organisations may be questionable. Yet, we felt that it was important to study organisations that we believed would have sufficient insight in the matter. Since risk and security are core activities within the bank industry, which they build their whole creditability on, we hoped that they could give us interesting answers. Finally, we were both present at every interview occasion, which increases the reliability since we were able to actively support each other and check that the answers of the respondents agreed with the questions.

3 THEORETICAL STUDY

In this section relevant theoretical background will be highlighted in order to get a general understanding of concepts and underlying theories that our thesis is based on. In the first part a general description of operational risk will be presented and then followed by a presentation of information risk and the concept of information risk management. The aim of the chapter is to give the reader a general comprehension of the topic that underlies our empirical study.

3.1 INTRODUCTION

As said before, risk can broadly be defined as the potential for events to cause future losses or fluctuations in future income (Marshall, 2001). Since a large part of the overall risks and perhaps also information risks, faced by firms ends up under the concept of operational risk we believe it is essential to present a brief introduction of the subject before moving on and give a more comprehensive presentation of the main focus of this thesis, i.e. information risk management.

3.2 DEFINITION OF OPERATIONAL RISK

There has been a lot of work done in ways of defining operational risk and ways of managing it. Within financial institutions operational risk can be defined as the entire process of policies, procedures, expertise and systems that an institution needs in order to manage all the risks resulting from its financial transactions (Hussain, 2000).

Marshall (2001) states that operational risk holds the risk resulting from operational failures, within back office or operations area of the firm. He also states that operational risk, from a wider view, is the variance in net earnings not explained by financial risks (Marshall, 2001). In other words Marshall (2001) advocates that operational risk can be defined as residual risk, i.e. everything that is not market or credit risk.

Hussain (2000) further specifies that operational risk include portfolio risk, organisational risk, strategic risk, personal risk, change management risk, operations risk, currency risk, country risk, shift in credit rating, reputation risk, taxation risk, legal risk, business continuity risk and regulatory risk.

Saunders (2000) advocates that the internal sources of operational risk are employees, technology, customer relationships and capital assets destruction. External sources are mainly fraud and natural disasters.

Another way of dividing operational risk into sub parts is to separate the two areas, operational leverage risk and operational failure risk. Operational leverage risk is the risk when the firm's operations will not generate the expected returns as a result of external factors, such as changes in the tax regime, in the political, regulatory or legal environment, or in the nature or behaviour of the competition. Operational failure risk is the risk that losses will be sustained, or earnings foregone, as a result of failures in processes, information systems or people. In contrast to leverage risk, the risk factors in failure risk are primarily internal. (FinanceWise, 1999)
(See figure 4)

Figure 4 Operational risk (FinanceWise, 1999)

Bessis (1998) looks at operational risk in another way. According to him operational risk can be divided into two different levels; the first level consist of technical issues such as when information systems or the risk measures are deficient, the second level has more organisational characteristics involving reporting and monitoring of risk and all related rules and procedures. Bessis' (1998) definition implies that a lot of the operational risk evolves from information technology. In the next section we will continue by presenting the concept of information risk management.

3.3 DEFINITION OF INFORMATION RISK MANAGEMENT

Theory concerning information risk management has not been easy to find, which have resulted in that this section covering information risk management is based on articles consisting of different viewpoints within the subject. During the study we have frequently come across concerned subjects such as information security, information risk, and information assurance. We have also taken a look at the governance of information risks, i.e. action plans used to manage these risks as well as at what company level the strategic information risk decisions are made. Together these areas can be said to underlie and create the concept of information risk management. In the literature, the definitions mentioned above are quite ambiguous but we will here try to separate and clarify them.

3.3.1 INFORMATION SECURITY

Information security is required because the technology applied to information creates risks (Blakley, et al, 2001). People traditionally associate information security with technology and most focus is put on technical aspects, such as different hardware and software (IAAC, 2003). Thus, the definition of information security commonly deals with it as a technical support function. The literature as well as companies working within the area has different explanations to what information security is about, but most commonly it seems to be solutions due to problems concerning technology. This is the definition we are going to stick with in order to be legible in our review of information risk management.

The protection of information might be concerned with more than just technical issues. In the next section we will discuss information risk, information assurance and also the governance and management of theses risks to create an all-embracing comprehension of different parts that might belong within the concept of information risk management.

3.3.2 INFORMATION RISKS

Organisations that are faced with complex information technology environments, deal with issues such as open systems, IT platforms, strategic exploitation of electronic integration, network interconnectivity etc. Such technology applied to information creates risk. But information risks are not only connected with technology. Information risks are associated with the disclosure, modification, unavailability or destruction of information, which is not only due to technical aspects, but also could be caused by human factors (Kotulic & Clark, 2004; Blakley et al, 2001). In other words, information risks have many technical elements, but the magnitude of risk is largely determined by non-technical factors, including business relationships and attitudes of the information technology users (eWeek, 2004). Gary Riske, who is information risk management partner of the US-based KPMG, emphasises in the same way, that information risk involves technology as well as processes and people in an organisation (Pardas, 2002). Examples of information risks might span from a former employee who brings with him important client information to a competitor, or carelessness and scarcity concerning routines, such as sending sensitive business specific information via MSN messenger or external threats such as automatic attacks from hackers playing around.

Since information risks include more than just technical issues, the traditional term information security with its technical approach, may not be the best applied. Instead a newly evolved

concept has emerged called information assurance, which is a more holistic description of information risks. We will briefly explain information assurance in the next section.

3.3.3 INFORMATION ASSURANCE

The concept of information assurance expands the content of information security by dealing with it as a business critical operational function, rather than as a technical support function (IAAC, 2003). Information assurance can be defined as:

> *A holistic approach to protect information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation* (IAAC, 2003).

This definition puts both the technical and the human factors along with strategic aspects in the centre of attention. Failures in information assurance are adverse events, which cause losses to businesses and therefore it is essential to build up protection against these potential events (Blakley, et al, 2001). Hence, in the next part we will address the concept of risk management.

3.3.4 GENERAL RISK MANAGEMENT APPROACHES

As presented earlier, an organisation is exposed to a staggering array of risks, whether they are information risks, operational risks or financial risks. A general procedure to manage risk, consist of five phases: identification, estimation, evaluation, response and monitoring (See figure 5).

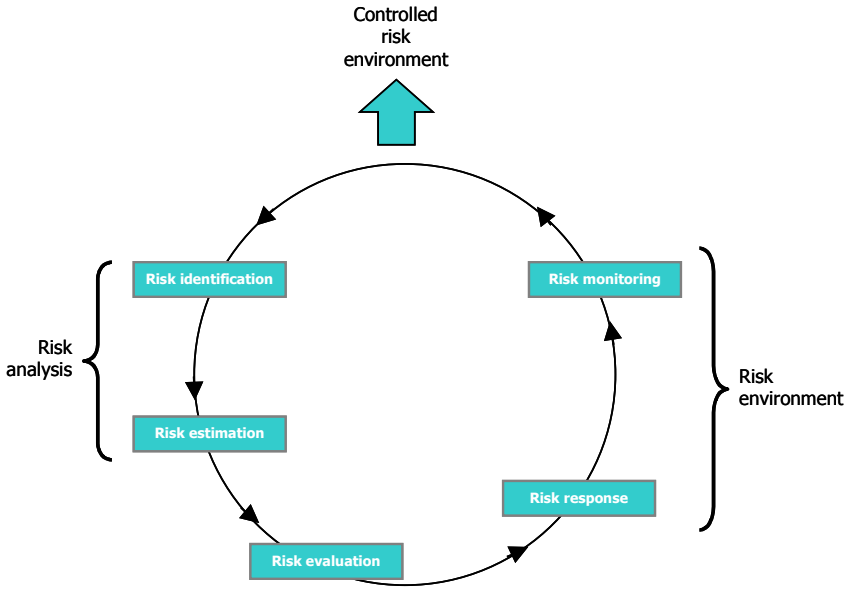

Figure 5 Risk management risk cycle (Baker, et al, 1998)

To obtain a controlled risk environment organisations need to first identify the threats that constitute risk to the organisation and then estimate the risk. These two steps comprise the important risk analysis, which every organisation should put time and effort to. Next step is the risk evaluation phase, which evaluate to what extent the risk might affect the business. The last two steps are about risk control and include risk response and risk monitoring. The organisations need to decide how to manage the risks and then monitor that the preventing actions comply with the intentions. (Baker, et al, 1998)

Regardless of how complex and varied the risks within the organisation are, a firm has four possible fundamental approaches to manage a given risk. A firm can avoid risk, reduce risk, transfer risk or retain risk. The first two approaches minimise a firm's overall exposure to risk and they are sometimes referred to as risk control. The two latter approaches are known as risk financing and the goal for those is to ensure that funds are available to cover losses that do occur after the application of risk control techniques. (Shimpi, 1999) We will briefly go through the approaches below.

3.3.4.1 Risk Avoidance

A firm can elect to abstain from investments with payoffs that are too uncertain (Shimpi, 1999). Thus, the risk can be avoided by not undertaking activities that are risky or by substituting less risky processes (Doherty, 2000). Each organisation has to draw a line between acceptable and unacceptable risks and the decision concerning where this line should be drawn depends on a combination of internal and external factors. Risk avoidance reflects each firm's need to maintain focus and pick its battles (Shimpi, 1999).

3.3.4.2 Risk Reduction

Risk reduction occurs through loss prevention, loss control and diversification. Loss prevention seeks to reduce the likelihood of a given type of loss occurring and examples of loss prevention measures include safety devices like smoke detectors and burglar alarms (Doherty, 2000; Shimpi, 1999). Loss control techniques are designed to reduce the severity of a loss, should it occur. Sprinkler systems and firewalls for example, limit the damage if a fire would take place (Doherty, 2000; Shimpi, 1999). Also, a firm can limit its downside risk of a project by inspections, closely monitoring its progress and regularly evaluating its efficacy, which is a loss control technique as well (Shimpi, 1999). Diversification provides a third mean of reducing risk, which has crystallised over the past half-century with Markowitz's development of the portfolio theory. It offers an opportunity to spread out the risk without sacrificing the expected return (Brealey & Myers, 2000; Shimpi, 1999).

3.3.4.3 Risk Transfer

The risk can also be transferred from one party to another better equipped or more willing to bear it (Shimpi, 1999). For example, the risk can be transferred to counterparty by purchase of an insurance policy or financial hedge (Doherty, 2000).

3.3.4.4 Risk Retention

Companies also retain a variety of risks, whether voluntarily or involuntarily, i.e. in an active or passive way. Voluntary risk retention reflects a conscious decision to absorb certain risk exposures internally, because it is the most cost-efficient way of addressing the risk. Involuntary risk retention occurs when a business fails to identify a given risk exposure and therefore bears the risk unknowingly. A risk neglected is a risk retained, or simply not insuring is retaining risk. (Doherty, 2000; Shimpi, 1999)

Having grasped the fundamental risk approaches we will now move on to explaining approaches to manage the information risks. This is however not done in a twinkling. Managing information risks can be done in varies ways depending on the organisation. (Baker, et al, 1998; Blakley, et al; 2001 White, 2003; Hussain, 2000). We will here touch the subject in order to provide a general understanding

3.3.5 INFORMATION RISK MANAGEMENT

As said earlier information assurance is about ensuring the availability, integrity, authentication, confidentiality, and non-repudiation of information. Information assurance can be said to be a risk management discipline (Blakley, et al, 2001; IAAC, 2003). Every organisation wants to push the information risk down to an acceptable level (White, 2003).

Following below are more specific approaches to how organisations should go about understanding, monitoring and driving down the level of information risks. Information risk management is much about policies**,** which describe "who should be allowed to do what" when it comes to information and information flow (Blakley, et al, 2001). According to a survey made by KPMG, information risk management is about enhancing the processes and controls within the business in order to better manage the information risks, which in the end will make it possible for the business to meet its strategic and financial goals. Kotulic & Clark (2004) advocate, in the same way, that the goal of information risk management is to maximise possible gain while minimising possible loss. The process must be a cost-effective, non-technology driven, value creation process that contributes to the overall effectiveness of the organisation.

To decide on optimal policies about information risk management the business could deploy a mix of organisational processes and technical mechanisms including categories such as *protection* which is about preventing adverse advents from occurring, some kind of *detection* which alerts the business when adverse events occur, *response* which deal with the consequences of adverse events and return the business to a safe condition after an event has been dealt with, and some sort of *assurance* process which validate the effectiveness and proper operation of protection. (Blakley, et al, 2001).

Examples of optimal policies and actions to be taken can be encryption to prevent eavesdropping, firewalls to stop unauthorised network access, traceability enhancements such as capturing and recording of all file transfers, web accesses, e-mail, instant messaging conversations and internet-based voice traffic (White, 2003). Unlike other assets, information can be stolen without being lost. It is not enough, therefore, to ensure that information remains available to those who are authorised to use it. Information access must also be denied to others, who are not allowed to see or use it (eWeek, 2004). According to Lövgren (2004) risk management is also about making the information available whenever necessary, regular assurance about the accuracy of the information as well as dealing with secrecy and confidentiality, i.e. who gets access to what.

In addition information risk management is about having a risk aware culture, educating staff about the information risks and then managing the staff, managing incidents to avoid reputational damage, and providing business partners with assurance about security (IAAC, 2003; Hussain, 2000).

An organisation that can best assure that its systems and information are secure, confidential, available, reliable and maintainable will create a new competitive advantage for itself (Xystros & Weber, 2001).

In the next section we will address the issue concerning who is responsible for the risk management within the firm. We will especially concentrate on the role of the risk manager and the top management's awareness i.e. their involvement along with their commitment in the matter.

3.3.6 RISK AWARENESS AND RESPONSIBILITY

There is a relationship between sound risk management practices and earnings growth as well as corporate reputation. Establishing a good risk management strategy is essential. Many employees

strive to improve the firm's profitability, but only a few devote their time to risk management. It is interesting to consider who is responsible for the risk management strategy. (Shimpi, 1999)

According to Computer Weekly (2004) there is a preference to cold-shoulder or ignore risk, rather than to plan for and manage it. Many chief executives cannot see how spending money on information risk management can create real business value. On the other hand, a combination of new regulations, corporate governance issues, and increased accountability has shaken managers into paying more attention to information technology and information risk strategies (Computer Weekly, 2004).

According to Shimpi (1999) the chief executive officer (CEO) is responsible for a firm's success in the market place and he/she is therefore considered to be its ultimate risk officer. By ensuring that adequate risk management processes are in place at the firm, the CEO can reduce the probability of a major corporate disaster and identify potential obstacles in an early stage. The CEO sets the basic tone for the organisation and just how much risk the firm will bear. Hussain (2000) also advocates that the board of directors play an essential role when it comes to corporate governance and information risk management. They should for example ensure that organisations structure, culture, people and systems are conducive to effective information risk management. All in all, executive management involvement is a necessary condition for the successful implementation of an information risk management program (Kotulic & Clark, 2004; IAAC, 2003).

A number of firms have recently begun appointing executives to positions such as chief risk officer (CRO) or "vice president, risk management", charging them with overview and coordination of all risk management activities. The CRO role is to develop and implement strategies that will minimise the adverse effects of accidental and business losses on the firm. In addition, everybody is a risk manager, thus the divisions managers must also factor risk into the various decisions they make. The managers who are responsible for committing a firm's resources to different activities should always consider the relevant risk. (Shimpi, 1999; Kotulic & Clark, 2004; IAAC, 2003)

4 EMPIRICAL STUDY

The empirical study consisted of four qualitative interviews with experts covering operational risk and information security within four major Swedish banks. Altogether we conducted studies with seven persons, namely Tobias Hummel (SEB), Kjell Holmsten (SEB), David Högberg (SEB), Erik Palmén (Nordea), Lars Sefastsson (FSPB), Kathryn Gee (FSPB) and Hans Peterson (Danske Bank).

4.1 INTERVIEW GUIDE

The interview questions arose from our problem definition and from our findings in the theoretical study. The purpose for the questions was to give as much input as possible to our previously stated problem definition. The questions are to be found in Appendix 1, structured after the following main areas:

Definition of operational risk management

The reason for asking question concerning the definition of operational risk is to obtain an understanding for the risk areas, which are regarded as operational risk. The aim of the question is to figure out whether information risk is one part of operational risk or if it is considered as a risk element of its own.

Responsibility

Our intention with questions concerning responsibility, within operational risk management, is to comprehend whether different persons are responsible for the different risk areas within operational risk, or if one person has the total responsibility. If information risk is considered as part of operational risk we wanted to conclude where the responsibility for information risk issues lay.

Definition of information risk management

When studying the literature several vague definitions concerning information risk management came across. By asking the respondents about their definition of information risk management we hoped to gain a better understanding for the content of the concept

Structure and responsibility

In order to obtain a thorough understanding for the information risk management we considered it important to ask questions concerning how the work within the risk area was organised and structured. Questions concerning responsibility were also essential in order to fully understand the structure of the information risk management process.

Risks and management

Our aim with questions concerning risk and management was to learn about the threats that constitute a risk for the banks. We were interested to know whether those threats and risks were of technical character or of organisational character, in order to conclude how the different banks truly perceived information risk. By asking question about the risk and the management of the risk, we might reveal if the respondents defined information risk in one way, but actually perceived it in another.

Trends

Based on the fact that the information- and knowledge society is continuously expanding and developing, we found it interesting to ask question regarding how the information risks have changed and will change in relation to the development.

Awareness, commitment and involvement

The theory emphasises the importance of the top management's involvement in the risk management process. Our aim with these questions was to find out how well committed and involved top management is in information risk management. We would also like to find out whether there is a difference between the awareness and involvement between top management compared to general employees.

4.2 FINDINGS

4.2.1 SEB

Respondents: Tobias Hummel, Operational Risk Control, SEB Merchant Banking, Sweden. Kjell Holmsten and David Högberg, MB IT Strategy Information Security, SEB Merchant Banking, Sweden. (for further facts about the bank, see appendix 2).

4.2.1.1 Definition of Operational Risk Management

According to SEB, operational risk is defined as all kind of risks that are not counterpart, market, strategic or insurance risk. The risk that the following conditions or events result in unexpected losses or reduced confidence in the Group:

Environmental factors such as reputation problems, supplier failure, natural disasters and criminal acts or, internal problems such as ineffective procedures, inadequate information systems and technology, non-compliance with regulations and legal agreements, fraud and other illegal acts committed by management and staff or other weak internal controls.

SEB's definition of operational risk is rather similar to Basel II (see appendix 6), although, Basel II does not specify how to treat compliance under the new accord. According to Tobias Hummel

it is difficult to rank the weight of different operational risks in an organisation. However, according to the Basel Capital Accord 80% of the risk capital should be put on trading related activity and 20% of the risk capital should be put on corporate banking. This seems plausible because of the fact that fraud within trading has been one of the largest causes of operational loss within the banking industry.

4.2.1.2 Responsibility

Philip Winckle is Head of Group Risk Control within SEB, with Lars Hansén being responsible for operational risks. Allan Palm is head of operational risk at the SEB Merchant Banking. Tobias Hummel works for Allan Palm within SEB Merchant Banking. Each department is responsible for the operational risks inherent in their respective business activities. Taking responsibility for your risks is according to Tobias Hummel the only possibility in trying to control them effectively. Each department and department manager is fully responsible for making sure that the operational risks are managed and controlled in a satisfactory way, on a daily basis and within established group guidelines. It is also a fundamental principle that all control functions shall be independent of business operations.

Operational Risks main responsibilities are identification, monitoring and measuring operational risks. It is important to check up on incidents and to discover potential weaknesses in the business. Developing tools for risk managing is also part of the overall responsibilities as well as making sure that the objectives of Basel II are implemented throughout the organisation. SEB also perform different disaster planning or worst case scenario analysis to find out alternative ways to run the bank in crises situations.

4.2.1.3 Definition of Information Risk Management

Information risk management as a term is not used at SEB, but Information Security as well as IT Security, are areas where SEB has its focus. David Högberg and Kjell Holmsten state that information security is 80% about attitude and 20% about technical issues. Thus, information security is mainly about educating employees in order to get them to understand the risks. They believe that trying to build away problems with technical solutions is more or less impossible and in addition it is rather impractical to work in such a complex technical environment. All in all, information risk is risks in relation to the availability, integrity, confidentiality and traceability of information.

4.2.1.4 Structure and Responsibility

Within operational risk there is a function called operational risk assessment, which works with cost analysis and probability analysis in relation to certain scenarios, such as the bank being

exposed to strong competition or a system breakdown during a certain amount of time. Information risks, focused on control of systems and technology, might be one part within this kind of operational risk analysis. But otherwise information risk is not a part of operational risk. Instead SEB has a Group wide staff function called Group security, which work on the overall group level, writing instructions and policies that form the "law book", regarding the handling and managing of information security. In addition to their work each division implement and apply these rules as well as monitor whether they are complied. David Högberg and Kjell Holmsten works within a group called MB IT Strategy Information Security, which is part of the Merchant Banking, and they help to implement the rules set by Group security. Information security works closely together with the bank's different business areas, ensuring that the particular business areas are safe. Kjell Holmsten is the manager of information security and David Högberg works together with him. As a complement, people within every business area, works with information security on an everyday basis. The ultimate responsibility obtaining an adequate Information Security situation lies on the System Owner of each system. Kjell Holmsten and David Högberg can identify areas of technical deficiencies and pass forward such matters to the IT security division, which takes care of the technical implementation. In addition the Group security deal with the matters on group level. All these three instances work together to secure the information in different ways.

4.2.1.5 Risks and Management

According to Kjell Holmsten and David Högberg the main risks that threaten the bank are those caused by external factors. When it comes to internal risk factors Kjell Holmsten and David Högberg emphasise the importance of having an environment where employees enjoy their work and do not perform precarious or intentional risky actions. There is a vital trade off between extreme control and less control; too much security is as dangerous as to little.

To secure the confidentiality within SEB the bank has an extensive framework with instructions concerning what is permitted and what is not. This framework covers everything information specific. The confidentiality agreement[1] also gives certain confidentiality protection and this agreement is valid for the rest of a person's life. It is not either allowed to use external webmail, instant messaging conversations or similar communication channels. There are certain rules regarding what kind of information that is legitimate to transfer via certain transfer channels. When it comes to the availability SEB has comprehensive contingency plans. If a system breaks down for example, the next goes up at the same second. Kjell Holmsten and David Högberg. also emphasise the shared drives, available for everyone within a particular business area.

[1] In Swedish, *sekretessförbindelse*

Backups are also taken on a continuous basis. To maintain the information integrity within the bank, the information is first and foremost, classified into open, intern, confidential and strictly confidential. Authorisation rules and rights rules is also part of the integrity assurance. The person who is main responsible for a certain piece of information, decides upon classification, authorisation and rights. In all company systems within SEB traceability is possible. Every action an employee performs is logged and the bank has the possibility to do check-ups regarding when, where and how an employee took action.

The Information security department within the Merchant Banking does not work with technology in any way, i.e. it does not put any resources into technical issues. Their capital is rather invested in issues like choosing and determining which option of A, B or C, is most secure and safe. Analysis and researches regarding such matters are both costly and demanding. However, the Information security department is of course communicating and cooperating with the IT division but the two divisions' responsibilities are different.

The awareness and knowledge concerning information risk management has increased a lot lately. Kjell Holmsten and David Högberg mean that the understanding among employees is sufficient at the moment. They have just run an extensive education, which is quite a new occurrence within information security area. The feedback has been very positive and the employees found the education very interesting. Information security seems to be an issue that really engages people today. Great attention and sympathy for the different information instructions exist within the bank, but it is nevertheless difficult to control that people are really complying.

4.2.1.6 Trends

The most obvious trend is that during the recent years SEB has increased and reorganised their Information Security activities to enable SEB to be more alert and meet the threats in a proactive and effective manner. Another trend, which Kjell Holmsten and David Högberg emphasise is the enormous increase in spam e-mails and viruses during the last years. They state that if this pace in information technology development continues it is going to be crowded on the Internet, which will increase the spam and virus attacks even more. It is not only a matter of computers, also smart telephones, PDA's and things alike need to be secured and protected. The employees are however rather aware of some of these risks. For example, employees are exposed to risks when using their, often unsecured, home computers for Internet activities and because of the risks they face at home they become aware of the same threats and risks in work related contexts.

4.2.1.7 Awareness, Commitment and Involvement

The fact that the Information security department as well as Kjell Holmsten and David Högberg exist is a significant initiative from the top management. The information security issues have, as said earlier, been emphasised considerable the last years and today every employee can be said to have information security as part of their work assignments.

Kjell Holmsten and David Högberg state that their position in this matter is somewhere in the middle. They are acting downwards, working together with the various business areas to secure the information, and also acting upwards with the management, discussing and reviewing initiatives and proposals. The two of them have the main competence within this field and they use it to saw seeds within top management, who gives approval or non-approval to project implementation at business level. It is important not to push new ideas and initiatives onto people, instead overall acceptance is a keyword in order to succeed.

4.2.2 NORDEA

Respondent: Erik Palmén, Head of Group Operational Risk Management, Nordea, Sweden. (for further facts about the bank, see appendix 3).

4.2.2.1 Definition of Operational Risk Management

Operational risk within Nordea is defined on the same basis as the definition in Basel II (see appendix 6), i.e. the risk of losses resulting from inadequate or failed internal processes, people and systems, or external events. In addition, damaged reputation is a part of operational risk. The main risk areas belonging to operational risk constitute information security including information technology security, legal risk, compliance risk, process risk and event risk. Broadly, operational risk can be separated into event risks and process risks. All risks are equally important. According to Erik Palmén at Nordea, the event risk has been emphasised a bit too much in Basel II and he believes it can be a problem of today that most people are talking about operational risk with an emphasis on the event risks/incident risk. Erik Palmén means that it could result in a misleading picture of what operational risks are. In addition, he also emphasises the importance of being aware of the border between risks and quality problems.

4.2.2.2 Responsibility

Erik Palmén is Head of Group Operational Risk Management at Nordea and his responsibilities lies within continuously developing and maintaining frameworks, models, methods and other prerequisites for the business, which could help managing the risks. He has a general overview of

the implementation of the framework and he takes specific action in alarming cases. In line with his work, every division manager is responsible for the risk at his/her division.

4.2.2.3 Definition of Information Risk Management

According to Nordea, information risk management is about managing and restricting the risks of deficiencies in information availability, accuracy, authentication, confidentiality, and non-repudiation.

4.2.2.4 Structure and Responsibility

Within Nordea it does not exist a specific division for information risk management. Instead the information technology security division, which is technically focused, work together with Group Operational Risk Management, to diminish the information risks within the bank. On an overall basis information risk management has grown in importance during the past years and it is now expected that every division manager are aware and manage the information risks. Information risk management is part of the operational risk management. 20 percent, i.e. one person out of five in the Group works with information risk management issues. Further, ten persons work with information technology security, which means that capital invested in information technology is greater than capital invested in more general information security issues. However, a total number of eleven persons working within this area do not give a completely proper picture of the situation. It is misleading to think that only one person out of eleven works with information security that falls outside the frame of information technology. It is rather a matter of traditional heritage to mostly approach those issues from a technical perspective. Lately the bank has studied the picture from a broader perspective, which have resulted in changes in the corporate governance model.

4.2.2.5 Risks and Management

The information risks within Nordea can vary quite much and it is therefore difficult for Erik Palmén to say what kind of risks that are the most dangerous and/or serious. Yet, three main risk areas can be said to exist. These are risks concerning the information availability, integrity and confidentiality. Traditionally a lot of management focus is put on the availability, whereas confidentiality and integrity is taken for granted. Although financial institutions have built their entire business on information technology, they have never been exposed to situations where the integrity has been seriously damaged. Instead the management tends to focus more on availability and the perception of "great IT problems" is still often connected to cases like the ATM:s do not work. An availability problem like this is of course serious but according to Erik Palmén integrity and confidentiality is taking up to little attention and should be looked further into. It is of course

great that availability issues are taken seriously but those issues can be really difficult to handle if everything else (read integrity and confidentiality) fails.

Real serious threats against information integrity are intentional actions, especially actions in order to seriously get to/affect the information, such as modifying the information about production or the backup information. The same goes for confidentiality; the real threats are the intentional actions. Within Nordea, confidentiality is sometimes negatively affected due to technology, such as a bug in a system resulting in specific information becoming available for an unauthorised person. Such errors occur, on the other hand, very randomly and are corrected before any actual breach in confidentiality occurs.

The greatest of all information threats are insider crimes. Since the bank environment is a main part of a country's overall infrastructure, big threats to the financial institutions and the whole society are terrorist attacks, i.e. intentional actions with long underlying planning. Banks are quite rewarding objects in this context. On the other hand, these threats and risks are extreme and are rare in Scandinavia.

To manage information risks concerning confidentiality Nordea have general rules and policies and they always act in the interest of the client. Confidentiality is the main selling product of the bank so confidentiality should be part of every employee's way of thinking. Clear rules are being set up to promote this view. According to Erik Palmén it is not optimal to have totally forbidding rules, it is rather a question about making sure that those who have responsibility, becomes aware of their obligations. At the time being Nordea is also developing a framework concerning rules and policies for the usage of the communication channels such as the intranet and e-mail accounts, in order to protect the confidentiality of the information.

Finally, the law surrounding the bank industry is so clear that if information does leak and the confidentiality is damaged, it is usually because of an intentional, hard-to-discover act. It is not possible to prevent information for leaking if a person really wants to leak it. However, it is a criminal act and cautions can be taken thereafter.

When it comes to the availability and integrity of the information, Nordea as a large organisation, has extensive resources to put into this issue. The bank is continuously planning and preparing for information availability or non-availability. To start with, the person who owns a specific piece of information is responsible to classify the information as open, internal, confidential or strictly confidential. For external attacks, firewalls and continuously updated virus protections are

available. The bank also purchase services from professional "hackers" who try to break in to the system in order to test the security. Nordea has audit trail, i.e. traceability functions everywhere within the bank, which is one of the basic demands and ideas in banking.

When a failure occurs somewhere in the organisation, it is probably caused by a great amount of mistakes made on different levels by different persons, and therefore it gets even more critical to ensure that all employees are aware of the information risks and what responsibilities they have. To ensure the risk awareness within Nordea, all employees get education in subjects covering both information technology security as well as information security.

4.2.2.6 Trends

When discussing the awareness of information risks it becomes clear that a couple of years ago information risks were mostly associated with virus, and they were conscious not to put in a "suspect" disk into a computer. Few bothered or knew about the information risk they were exposed to when, for instance, sending e-mail. Today the situation is different according to Erik Palmén. The information risk awareness permeates the whole organisation and even the top business levels are involved. Erik Palmén believes it is a question about culture, i.e. it is essential to have a, so-called, risk culture within the organisation. Risk culture should be seen as a key concept. The information risk awareness within Nordea has, without question, increased the past years, which could be seen as a positive trend.

Erik Palmén further stresses that there are especially two causes to the increased focus on information risk management. First, the general development in the world has made information technology go from being specifically applicable to only certain business areas, to being more high-tech and complex but at the same time more general and user friendly. This has resulted in that more or less every business of today base its business on information technology. Everyone, everywhere within the business, transfers information. Based on this fact, Erik Palmén states that it is no longer possible to monopolise information related issues to be only of technical character. Second, when the debate about operational risk evolved in the banking industry a few years ago and operational risk units were created, information security was seen as a closely related matter, and therefore attention was put on those issues as well.

Erik Palmén advocates that during the last years increased knowledge and understanding for information risk management has arisen. Every level and division within the organisation are supported by information and it is essential to further get the business managers to understand the importance of investing capital into information risk issues and not merely on technical

aspects. It is not possible to regard the matter as a simple "IT-issue", which the "IT-department" has to deal with. Instead a more all-embracing perspective of the information risk management has to emerge. The IT-department, on the other hand, has to adjust to a new role of being one stakeholder among many in the field of information security. It is difficult to keep up with the pace of this trend but at the same time it is unavoidable and managers have to act upon it. At Nordea, Erik Palmén is something of a missionary working on Group level. At the time being, documents containing recommendations and policies for the risk management are revised. Additionally, lately a number of different units within Nordea have started to develop structures and a common language, rules and policies concerning information risk management, which is an initiative originating from the people working with operational risk management. However, Erik Palmén stresses that the operational risk management division does not want to monopolise the information risk issue, only promote it.

In the future it is impossible to avoid questions concerning information risks and Erik Palmén predicts that the matter will take up more time and effort in the future. Further, he stresses that the world keeps on moving towards an information and knowledge society and this fast developing trend is not going to change direction. Erik Palmén believes that financial institutions of today will probably give different answers within the subject of information risk management. But the information risk management trend is going to become more visible within a short time period, and it will increase the information risk awareness within most banks.

4.2.2.7 Awareness, Commitment and Involvement

In Nordea "missionaries" exist on every level in the bank, involved in the area of information risk management. The commitment is good among employees and they tend to quickly grasp the importance of the issues. The employees easily understand the risk since they work with information on a daily basis. It is quite straightforward to build up involvement and commitment from below. The top management thinks more in terms of information technology security and rely on the information technology division to take care of those issues. According to Erik Palmén the work concerning the awareness of information risk management has come half ways, which is positive. The commitment is nowadays growing more or less from every direction within the bank, which indicates that the culture is evolving in a sound direction.

4.2.3 FÖRENINGSSPARBANKEN

Respondents: Lars Sefastsson, Head of Group Operational Risk, Kathryn Gee, Specialist Group Security, FöreningsSparbanken, Sweden. (for further facts about the bank, see appendix 4).

4.2.3.1 Definition of Operational Risk Management

FöreningsSparbanken's official definition of operational risk, set by the Board of directors is, "the risk of direct and indirect losses resulting from inadequate or failed internal processes, people and systems or from external events". The bank strives to be as close as possible to the Basel II definition (see appendix 6). To put it simple, Operational Risk can be defined as; every risk apart from market and credit risk.

According to FöreningsSparbanken there are several dimensions to look at concerning what areas that belong to operational risk. One way is to study it from a perspective of different risk areas. In this case, FöreningsSparbanken discuss four cause-driven risk factors: personal, processes, IT/system and external. Specific sub areas exist within the frame of those four main areas where information security is one important part. The other perspective focuses on preventing and decreasing operational risk in relation to certain organisational business areas.

4.2.3.2 Responsibility

Lars Sefastsson is Head of Group operational risk, senior vice president. FöreningsSparbanken has a central risk function, but apart from that the bank also has local Operational Risk control functions at business unit level. The bank's view of operational risk control is that it should be carried out as close to the core activities as possible, i.e. on a local level. In that way the bank is very decentralised, and in every business unit and subsidiary there are people working full time with operational risk management. The central risk control, which Lars Sefastsson is in charge of, has the general responsibility for operational risk.

Physical security is also an evident component in the context of operational risk, such as ATMs that are blown up, banks getting robbed and so on. FöreningsSparbanken has staff, on local level, occupied with these kinds of matters. The department for Human Recourses also possess a great responsibility when hiring trustful and loyal people, which is vital in this context of operational risk management.

On Group level, FöreningsSparbanken focuses on operational risks factors that have potential to "make the bank shiver". Information technology is an important factor. The bank is totally dependent on information technology, if the systems or communication stop, then "the bank stops". Hence, extensive focus is put on the issue.

Lars Sefastsson's main responsibilities are to coordinate the Operational Risk control from a Group perspective, define standards and plan in order to make every employee work in a similar

manner. The central Group Operational Risk function also drives the development of new methods and techniques, which is an important part of his work assignments. In addition information and education as well as positioning to the new Basel II regulation, keeps him busy.

4.2.3.3 Definition of Information Risk Management

FöreningsSparbanken does not use the term information risk management. FöreningsSparbanken have not been able to identify a short, easy definition in any literature. Instead their definition is based on the standard definition SS-ISO/IEC 17799[2]. According to this standard, information security includes confidentiality, i.e. guarantee that the information is available only to those that are authorised to access it and have the right to use it. Further, integrity is included in the concept, i.e. protection of the information, in order to keep it accurate and complete. Availability is another part of information security, which guarantees that the users have access to specific information when they need it. Finally, traceability is also an important part of information security; it deals with the possibility to identify and store actions carried out. Information security includes physical, logical and system security according to FöreningsSparbanken. The bank policy, which comprises all security within the bank, state that information security, involves risk within the whole information cycle[3].

4.2.3.4 Structure and Responsibility

Kathryn Gee belongs to the Group security, which is a function straight under Chief Security Officer (CSO). Her specific responsibility is information security on Group level. Information security within FöreningsSparbanken is not a question of the work of one specific business division, thus it is function on Group level. On this level other risk issues are also handled. Four persons work with information technology related questions on Group level. They develop a framework of rules and policies in order to manage the information risk. The basic idea is that information security must be a part of the daily operational risk management, which imply that the responsibility falls on every employee and becomes a part of his/hers every-day work. Apart from the framework there is other available support for the risk management such as education and written reports. The bank also has a control and compliance function, which follow up the processes within a division or a part of the business. It is not possible for every manager on all

[2] Swedish Standard Institute develops standards to help organisations become more efficient and profitable. SS-ISO/IEC 17799 is a management system for information security, which provides the organisation with guidelines for management of information security.
[3] The information cycle can represent a continuous process involving never-ending input, processing, storage, retrieval, manipulation, heuristics, variable output, and data exchange (http://appling.kent.edu/ResourcePages/LTStandards/Chart/infocycle.html)

levels to know every single policy and recommendation in the framework; therefore recourses are invested to support managers in their daily work.

4.2.3.5 Risks and Management

Kathryn Gee and Lars Sefastsson advocate that one large risk that might threaten the bank is the overall infrastructure of the society (energy power, telecom, etc). They claim that since the dependence on information technology is increasing, becoming more complex, and the need for specialists and experts is increasing, the bank face more risk. The human being also constitutes risk since he/she is interpreting complex information everyday. The information can be misinterpreted which influence and increase the risks.

Information confidentiality is always something the bank has to balance with availability. Since information is transferred in and out of the organisation, it has become difficult to preventing business sensitive information from ending up in the wrong hands occasionally. A lot of the information used in a bank, such as information regarding different kinds of financial purchases etc., can be extremely business sensitive instantaneously, but of no interest a few hours later. It is very difficult to rank the risks due to importance. The question of what is most serious is always difficult to answer. For example, if a customer receives wrong information when he/she logs in to his/her internet bank, or if information about a customer leaks out from the bank, is hard compare and rank. However, they further state, that if they have to choose, confidentiality is probably the most important risk issue within the bank.

FöreningsSparbanken has of course, like other banks, many different business partners such as suppliers, clients and consultants. Those business partners are tied to the bank by standard contracts, which make them part of the bank as an extensional unit. Therefore the same rules regarding confidentiality apply for them. Some business partners have special contracts based on specific risk estimations.

Contracts and agreements also exist for the employees within the bank. Yet, if an employee wants to take with him information it is hard to prevent and discover. It is difficult to protect the business from an intentional act. It is important to work with authentication and access rights within the bank, and FöreningsSparbanken put a lot of effort in such issues. As a manager you have the responsibility to make sure that the employees beneath you only have access to the information he/she needs to carry out his/her work assignments. Also, it is every manager's obligation to look after that the employees follow the framework. Yet, trust is a basic idea. Managers could perform check-up and monitor every step that employees take but that is not

really the "Swedish way" of doing business. Traceability is an important part of the information risk management work, since it makes employees aware of the possibility to monitor and follow up on incidents.

Within FöreningsSparbanken an unwritten rule exists declaring that as employed by the bank you are not allowed to talk about anything concerning the bank's businesses and customers. Apart from that three classifications exist within FöreningsSparbanken: open, internal and confidential. According to Kathryn Gee and Lars Sefastsson it is always a trade-off between risk and benefit when classifying information. Classifying the information to hard might result in that it does not get available for everybody that needs it.

When it comes to different transfer and communication channels, FöreningsSparbanken trusts its employees only to send e-mails and internet surfing in work related contexts. It is an underlying fact that employees should separate work and spare time. However, Kathryn Gee and Lars Sefastsson imply that the bank could probably be better at providing employees with information concerning how they are permitted to transfer information. They have noticed that the employees who understand the risk included in a certain action take specific precautions, such as sending information encrypted or with special delivery. Others that do not have comprehensive understanding about the risks are thereby not taking necessary precautions. Recommendations concerning such issues are however clearly expressed in the framework.

As mentioned before it is the responsibility of every manager of a specific division to look after the information availability. As an employee, you should have access to the information you need, but it is difficult to set limits concerning the access rights. It is not uncommon that an employee receives more access than he/she actually needs, so the manager has the responsibility to follow up and see to that employees do not exceed their authority.

FöreningsSparbanken also has advanced protection for external attacks, but they emphasise that it is not only technical protection or systems; it can be human beings, organisation structures or policies securing the information.

Information is everywhere in the bank. Information risk is an area where both effort and capital is invested, which involves continuous work, with different focus depending on the current threat image. However, it is not always easy to stay on top of things, since the risks changes so quickly. Competence can sometimes be complicated to find within the bank and therefore FöreningsSparbanken consults outhouse specialists from time to time.

4.2.3.6 Trends

Discussing trends, Kathryn Gee and Lars Sefastsson addresses the fact that everything nowadays has become much more technological, i.e. more or less all activities within the bank are supported by information technology. In other words, the whole business is built on information, knowledge and competence. Company value today consists of intangible assets rather than tangible assets, which of course results in a greater focus on information risks and studying concerned questions from new angles.

A few years ago FöreningsSparbanken, together with a few other banks, had comprehensive ideas about the so-called electronic society. However, after implementation it seemed like people wanted to keep their physical money. Nevertheless, FöreningsSparbanken believes that payment means of electronic kind will become more and more common in the future.

The question concerning client information is also addressed. The trend is moving towards obtaining better and better data about credit holders, and on the basis of that it becomes possible to draw more valuable customer information out of the data. The bank can thereby be more specific in their risk estimations. Also, achieving more information gives the bank the opportunity to be more precise and accurate when determining what actions to take to prevent risks. It is an ongoing progress!

4.2.3.7 Awareness, Commitment and Involvement

The Chief Executive Officer (CEO), the board and the management are well aware of issues concerning information risk management. The top management of FöreningsSparbanken are both involved and committed and extensive resources are put on the topic. They also follow up and evaluate investments. The strategically responsibility is an obligation for the top management. FöreningsSparbanken has a Chief Information Officer (CIO) within the top management who works parallel to Kathryn Gee's superior. The employees under the CIO develop solutions and real action plans for the framework and policies that Kathryn Gee, in turn, writes down and work with. The CIO could be said to be the strategic link between the traditional data/IT division and the overall business activities. This kind of top management governance did not exist five, six years ago according to Kathryn Gee and Lars Sefastsson.

4.2.4 DANSKE BANK, ÖSTGÖTA ENSKILDA BANK

Respondent: Hans E. Peterson, Vice President - Security, Danske Bank, Sweden. (for further facts about the bank, see appendix 5)

4.2.4.1 Definition of Operational Risk Management

Our representative from Danske Bank briefly defines operational risk as the leftover after credit risks, market risks, political risks and opponent risk. Or to quote Hans E Peterson, Danske Bank:
Operational risk is the one thing left over, when everybody else has chosen the area they find most exiting and interesting.
Operational risks may however have several dimensions, according to Hans E Peterson. A large division in Denmark, within the Danske Bank Group works with the Basel II perspective, i.e. statistics concerning risk exposures for calculating the capital base of the bank (see appendix 6). In addition there are also people working with operational risk on a daily basis concerning the everyday bank business.

According to Hans, the question concerning what kind of areas that belong under operational risk is rather difficult to answer. He prefers to rather study what kind of threats that belong under operational risk. Those threats result in risks and the causes to risk can broadly be defined as internal and external causes. These two factors can be viewed as columns in a risk matrix where the first row consists of people who might constitute a risk due to the actions they take. This first row can in turn be separated into intentional actions taken such as robbery or fraud, and unintentional actions taken such as errors or thoughtlessness. The two next rows consist of technology and environmental events such as flood, earthquakes or thunderstorms. All these areas represent a framework, which falls within the assignments of the people working with operative risks.

To quote Hans E Peterson, Danske Bank:
Safety is not a work to be done, rather something that is to be achieved. If unwanted events or unknown events do not lead to damage, then safety exists.

4.2.4.2 Responsibility

As said above, the responsibility concerning operative risk within the Basel II regulations belong with the division in Denmark. When it comes to operational risk on a proactive base within the bank, Hans E Peterson is Chief of Security. That means that he looks after the overall security of the bank. However, the responsibility concerning operational risks lies on each manager on each division of the business. The division managers are responsible for the security of their division. Hans E Peterson main responsibilities and assignments are supporting and analysing. He helps out by putting together different tools and method for assurance of the safety. He sees himself as a kind of a data exchange switchboard. The information that he is managing can be divided into three main headings:

1) Information without any special security value, which is sorted out and handled minimally.
2) Incidents and events that need to be taken care of immediately and therefore are passed over to concerned manager straight away.
3) Other information, input from the proactive security work is analysed in consideration to changes in threats, essentiality and risk and later packaged into proactive action plans.

4.2.4.3 Definition of Information Risk Management

According to Danske Bank, information can be found almost everywhere such as in computer systems in archives, shelves and drawers. Information risk management is about availability and non-availability, i.e. the information should be available to who ever need it, but at the same time unavailable for those that does not need it. Confidentiality is included as a large concern in this matter as well. Information risk management is about keeping the information accurate for the specific purpose, i.e. correct and complete. Traceability is also included in the concept concerning keeping track of where the information first was created, where it has been and is stored as well as who has been modifying it.

4.2.4.4 Structure and Responsibility

Within Danske Bank the information risk management is part of the operational risk management. Danske Bank does not have an information risk division in particular. They have a chief of security, Hans E Peterson, and together with him each manager is responsibility for the information risks at their particular division. The bank also has an IT security division, which works with hardware and software. The main focus of the security is put on deficiency and errors compared to how much time and effort that is put on internal threats.

4.2.4.5 Risks and Risk Management

Danske Bank claims that there are two dimensions of risks and threats, the seriousness and the magnitude. It is difficult to rank different risk areas, they are all very important to consider, but there are some threats the bank pays extra attention to. To start with, errors and deficiencies in management, technical systems, development and usage might cause serious damage. Both technical and manually risks are important to be aware of. Deliberate misuse of information such as people using information in an inappropriate way, or simply steal company specific information constitutes a risk. Further, different types of interference, i.e. external attacks such as viruses, trojans or hackers messing about as well as specially developed "bad systems" that sniff passwords or codes are also a large risk factor for the bank.

To manage information risks in relation to leakage, Danske Bank has for example several agreements and contracts with its business partners and confidentiality commitments are always signed. Also, instructions, agreements and correspondence are protected, since it is company-classified information. Agreements and contracts exist for the employees as well to protect the bank from leakage of information. In addition the bank can rely on help from the law about bank confidentiality, which states that it is always a criminal act to spread information about customers and employees. Thanks to the law, the bank only has to remind the employees about the contracts and agreement, not to monitor them in a further extent.

To ensure that information does not leak from the personal computers Danske Bank has decided that employees are not administrators for their own computer. Instead an employee needs to ask for permission if he/she wants to install a new application. In this way the bank has total control of the existing applications and the potential risks involved having those. It is neither allowed to use e-mail in correspondence with clients since Danske Bank believe that e-mail is comparable with wide-open postcards or fax. Instead correspondence with clients can be complete through the Internet bank, where mailbox functions exist such as webmail. Secured communication through telephone is also possible since the user can be verified through a digital code.

Discussing the availability of information within the Danske Bank, the basic idea is that several people know about a clients business, so if the key person is away for a day, someone else can easily take over the client account. In this way the bank tries to diminish the need for key persons. From a technical perspective, the availability of information is secured by having two data centres several kilometres apart as well as mirroring the data. Several operators are also always involved in the process of keeping the information available.

Danske Bank also has rules and policies concerning authorisation and rights for accessing information. It is important for an employee to get access to the specific information he/she needs for his/her work, but it also important to deny access to the information he/she do not need in his/her work. However, it can be difficult to technically restrict and draw a line between authorisation and rights, which have resulted in quite general authorisations but rather restricted rights. When it comes to potential external attacks and modification of the information, the bank secures itself by having different protection such as traditional firewalls etc.

In addition every transaction within the bank is traceable, which is possible since every employee have an identity when logged on to a system. A special group once in a while checks the log to make sure that people follow the rules and existing policies. However, the traces from the

employees might sometimes be misleading, which is a problem. The policies concerning traceability state that an employee should always be logged onto the computer he/she is working on at the moment, but during a busy day in the office, the rule is usually ignored which results in traceability gaps. It takes to much time to change users in the systems and the fact that the client should receive fast and efficient service is always put in the first room.

At the time being, employees at Danske Bank get technical education about the security installations one time per year. Apart from this training, they always have the opportunity to reach the latest information via their intranet. However, Hans E Peterson advocates that it on a general basis is easier to obtain resources for technical issues, such as implementing a technical solution in order to "build away" threats. Investing in technical issues is visible to a further extent and therefore easier to motivate. Investing money in time, such as education is instead rather invisible and harder to encourage.

The overall risk alertness within Danske Bank is extensive. To start with the awareness of robbery and fraud is widespread among employees. Lately the employees have become more aware of information risks as well, especially the possibility of worms or trojans damaging the information, which has made them more cautious. Employees continuously get education concerning risk awareness, not only concerning information risks but also about other risk issues. The work within the security area has large support among both employees and managers. Employees working in the offices get education twice a year concerning burglar alarms and other alarms.

4.2.4.6 Trends

In the beginning of 1990 a so-called information security policy was established at the bank. This policy was further developed into a more all-embracing security policy, including policies for all risks faced by the bank. The overall perception of all concerned risks is the same within the bank, therefore this policy still works. Although information security has been a part of the overall security within the bank for almost 14 years, the concept has diminished a bit lately. There were a lot of discussions in the beginning concerning information security but the basic idea has disappeared to some extent. Nowadays more focus is put on IT and technical issues. Less on information and information risk management. People tend to forget where the real threats are hidden. There are also a lot of discussions concerning standards like ISO 17799/9000/14000 and so on, but those standards are mainly about management systems regarding information security, quality and environment. The standards that are information technology focused are still technology intensive and expressions like computers, hardware and software are frequently reoccurring. This is of course important within the area of information technology security but

no attention is put on information and information security, and security as a quality. According to Hans E Peterson the quality of information risk management, as it appear in the public debate, is not at all sufficient. Everybody needs to start concentrating on more than just information technology and other technical issues. It is time to start thinking about questions such as, why protection need to be implemented, what are the intentions, what is important for us to protect? Hans E Peterson advocates the importance of returning to the concept of information security, which the bank developed in the beginning of 1990 and put less time and effort into information technology security.

4.2.4.7 Awareness, Commitment and Involvement

On a policy basis information risk management is integrated on every level within the bank. Danske Bank emphasises safety, quality and profitability within the area of information risk management. The top management is interested in questions concerning information risk management and put time and effort into those issues. However, they are not directly involved in the risk management process. Direct strategic directives are not received from the top management, although their awareness of information risks is extensive. When it comes to propose and suggest actions to be taken they are not actively involved. They rather expect the employees to inform them if some risk management process is not sufficient.

5 ANALYSIS

The main questions specified in the problem definition of this thesis lies as an underlying incentive for the research. In order to fulfil the aim of this thesis an analysis of the concept information risk management, the engagement and awareness of information risk management, as well as other surrounding areas, will be undertaken in this chapter. It is now time to compare the results with concerned theories.

5.1 OPERATIONAL RISK MANAGEMENT

According to the literature operational risk are viewed from a bit different perspectives. The overall perception of the concept is however relatively the same. On the basis of our findings, the view of operational risk within financial institutions appears to be very similar.

As mentioned in the theory section, operational risk might be specified to include portfolio risk, organisational risk, strategic risk, personal risk, change management risk, operations risk, currency risk, country risk, shift in credit rating, reputation risk, taxation risk, legal risk, business continuity risk and regulatory risk. (Hussain, 2000). Our respondents do mention some of these areas but not in the same specific manner. Instead they explain and define operational risk by excluding other, not belonging, risk areas. For example, Marshall (2001) state that operational risk on a general and simplified basis can be defined as residual risk and our empirical study show that operational risk within financial institutions is defined in the same way. To exemplify, definitions of operational risk can look like the following (See figure 6):

Operational risk is defined as all kind of risks that are not counterpart, market, strategic or insurance risk. (SEB)

Operational risk is the one thing left over, when everybody else has chosen the area they find most exiting and interesting. (Danske Bank)

Operational risk is every risk apart from market and credit risk. (FöreningsSparbanken)

Figure 6. Operational risk definitions

These definitions are rather vast and unspecified. When studying the concept on a more in-depth basis the literature emphasis that operational risk can be defined as the entire process of policies, procedures, expertise and systems (Hussain, 2000) and most often is viewed from a perspective of where the risk originates. The interview respondents have a tendency of dividing operational risks into different areas as well. For example, SEB emphasises that operational risk is the risk of losses resulting from inadequate or failed internal processes, people and systems, or external events. In the same way, Nordea states that operational risk is the risk, which is a result of direct

and indirect losses caused by non-objective internal routines, human errors, and erroneous systems or because of external events. FöreningsSparbanken advocates that operational risk is due to environmental factors and internal problems. This way of dividing up the risks agrees with Saunders (1998) internal and external approach to the issue. Since operational leverage risk are caused by external factors and operational failure risk are caused by internal factors the respondents way of dividing operational risk follow the approach of FinanceWise (1999) as well.

However, Bessis way of separating operational risk into one level consist of technical issues and a second level consisting organisational characteristics is not a common way to divide the risks according to our empirical study. Both those factors are of course believed to be part of operational risk, but the separation is not done in this particular way.

Further, Danske Bank has created a matrix of the risk areas included in operational risk, where people's intentional and unintentional actions are emphasised as well as technological and environmental factors. Although the different risk areas have been identified before, the specific matrix approach has not been found in the literature. Also, the way of stressing intentional and unintentional actions has not been pointed out in the literature.

To sum up, all the banks have, as said earlier, almost the same perception of operational risk. It is, however, interesting to study Danske Bank's matrix of operational risk since it ties intentional and unintentional actions within the context of people technological and environmental factors in an understandable way. It is notable that information risk management, on an overall basis, is perceived, as part of operational risk management, but it does not seem to be a specific business area with clear frames. It is rather floating and permeating all areas within operational risk management as well as risk areas outside the frame of operational risk. Since information risk management does not easily fall into any well-defined risk area, it is placed within operational risk management in the same way as other ambiguous risk factors are.

5.2 INFORMATION RISK MANAGEMENT

5.2.1 DEFINITION

In the theory chapter, information risk management is either seen as a concept dealt with as a technical support function or a concept which focuses more on risks related to information availability, integrity, authentication, confidentiality, and non-repudiation (IAAC, 2003).

According to our findings, the concepts, apart from information security, are not used within the financial institutions represented by our respondents. To clarify, the expressions stated in the literature are not commonly used in reality. Instead it seems like everything relating to information risk falls under the term of information security. When discussing the content of information security it becomes obvious that the respondents include a lot more into this concept than we found in our theoretical study. All our respondents have nearly the same perception concerning what constitutes a threat to the information and how to secure the information. They all agree on that information security is about risks in relation to information availability, confidentiality, integrity, authentication, and traceability. These factors, apart from traceability, are mentioned in the literature under the concept of information assurance, so although the respondents define it as information security, they do not perceive it as a technical support function but rather from a comprehensive holistic business risk approach. What we in the theory section call information security is rather comprehended as "IT" security, i.e. closely related to technical aspects.

It is obvious that no common definition of this concept exist, which accordingly often results in confusion over what the concept stands for. Different expressions frequently get mixed up and it is difficult to grasp what one concept or another refers to, without an in-depth analysis of every organisation's perceptions and expressions. However, all respondents, in the end, discuss the same risk issues although they define them differently. It is rather apparent that they have the same understanding of information risks.

5.2.2 STRUCTURE AND RESPONSIBILITY

According to the theory it is a good idea to appoint risk officers within the organisation in order to obtain and enhance the overview and coordination of the different risk management activities. Also, to be able to minimise the potential risk causing losses of the firm, the risk officer should develop and implement risk strategies and frameworks (Shimpi, 1999; Kotulic & Clark, 2004; IAAC, 2003)

To start with, all banks, apart from SEB, consider information risk management to be part of the operational risk management. Nordea do consider the management of information risk to be part of the overall operational risk management, and the bank does not have a specific division for information risk management. The information risk issues are dealt with on Group level within the area of operational risk management. This implies that one person is assigned to be responsible for the operational risk management and thereby the information risk management

on an overall basis. The assignments for the overall risk manager consist of development and maintenance of different prerequisites for reducing the risk level within the businesses. A close cooperation with the information technology security division is carried out in order to diminish the information risks within the bank.

FöreningsSparbanken has almost the same approach, but within the bank the person working with information risk related issues on Group level, does not work with operational risk issues. The assignments also consist of development and maintenance of different prerequisites for reducing the risk level within the business. Also, four other persons assist on the same level, being more focused on information technology related issues.

Danske Bank has a bit different approach of how to structure the information risk work. The bank does neither have an information risk management department nor an operational risk management department in Sweden. These units do exist, but are located outside Sweden. Instead the bank has assigned one person to work on an overall basis with the security of the bank. The work assignments of this person include everything related to security, covering for example issues such as information security, burglary security, physical security as well as other organisational security. For assistance in technical issues the IT security division is available.

SEB, which does not consider information risk management to be part of operational risk management, also has a Group security approach. On this level, development and maintenance of the general risk policies and strategies are carried out. In addition the bank have an independent information security division. Two persons work within this area and their work is carried out in a two-way direction, both upward towards Group security and downward towards all business areas. In this way their work assignments include implementation of the framework as well as to follow-up risk management actions. The information security division cooperates with the Group security and the IT security division in order to handle the risk issues within the bank

It may be hard to compare the structure and organisations of information risk management within the different banks. Their organisational structures vary. We believe it is more interesting to note that they have all taken care of the information risk management issue in a sufficient way. However, we do have some comments to the different bank approaches. To start with, Danske Bank has assigned a person to be overall responsible for the bank's security, which includes several factors outside the frame of information risk management. This is a rather comprehensive task where information risk management may not be in the centre of attention around the clock.

A better approach might be to assign a person only to focus on information risk issues, which is exactly what the other banks have done. We especially believe in the approach of SEB which not only have a person on Group level who is responsible for these issues, but also has assigned two persons "in the middle" who work together with all the business areas as well as upward together with the Group.

Although the four research objects in point have different structure and organisation to their information risk management, they all apply an all-embracing responsibility approach, i.e. the banks have at least one person who is, more or less, assigned responsibility for information risk issues on Group level. This approach goes well in hand with the theory concerning the importance of appointing a risk officer with main responsibility for the information risk management process.

In the theory chapter, we also emphasise the importance of having risk managers within all business areas (Shimpi, 1999; Kotulic & Clark, 2004; IAAC, 2003). The banks apply this philosophy entirely. They are all very carefully pointing out that the definitive risk and the responsibility concerning security should be decentralised and lie within the work of the manager of respective business area.

5.2.3 RISKS AND MANAGEMENT

As already mentioned, information risk involves technology as well as processes and people in an organisation (Pardas, 2002). These ways of distinguish information risks consent with the way the respondents in our study experience threats towards the banks. The respondents bring up a number of important information risks threatening the banks, but they especially mention a few that we will discuss a bit further.

The main threats according to our respondents seem to be risks in relation to information availability, integrity and confidentiality. Errors and deficiencies in management, technical systems, development, usage and policies are mentioned risks that might cause serious damage. The employees themselves constitute a risk since they are interpreting complex information everyday and they might do it improperly. Such actions are still unintentional. A larger threat to the banks is intentional misuse of information, which is harder to control or prevent. Different types of external interference and attacks are also a risk factor, but they are often not of serious nature.

In the theory chapter we bring up four possible fundamental approaches to managing a given risk. The first two approaches minimise a firm's overall exposure to risk and they are sometimes referred to as risk control. The two latter approaches are known as risk financing, which aims at ensuring that funds are available to cover losses that occur after applying risk control techniques. (Shimpi, 1999) It might not always be obvious to where different information risk management techniques belong within the four fundamental approaches. A general viewpoint would be that information risk management is mainly about risk control, i.e. risk avoidance and risk reduction. By implementing different kinds of technical protections, organisational rules and policies the organisations are trying to avoid the risks, or trying to reduce the risks as much as possible. Part of the information risk management could also be said to belong under the risk retention approach. Information risk might be retained due to the knowledge of when trying to manage some risk, further risks might occur. Information risks may also be involuntary retained if the organisation fails to identify any information risk and continues staying unaware of it.

To decide on optimal policies about information risk management Blakley et al (2001) stated that the business should deploy a mix of organisational processes and technical mechanisms including categories such as protection, detection, response and assurance. The actions that the banks are taking to secure their information fall under those categories although the boundaries between them are rather indistinct. According to our empirical study, protection, detection, response and assurance seem to go hand in hand and together they constitute the foundation of the banks' information risk management process.

To start with, according to Lövgren (2004) risk management is about making the information available whenever necessary. The banks are always continuously planning and preparing for information availability or non-availability. From the technical perspective, the banks have comprehensive contingency plans of all kinds. Some of the banks are also trying to diminish the need for key persons. This makes it possible to continue working although a central person is away, which secures the availability. The banks are also taking different kinds of technical precautions such as installing firewalls and virus protections in order to secure, especially the availability, but also the integrity, from being damage by external attacks.

According to Blakley, et al (2001) information risk management is much about specific policies**,** which might decide "who should be allowed to do what". All the banks we have interviewed have an extensive set of rules, policies and agreements. They also have rules concerning information classification. The information are usually classified into open, internal confidential or strictly confidential. In addition, authorisation rules and rights rules exists. By setting up rules

like this the employees have access to the information they need in order to carry out their work assignments. In this way, the banks secure the information availability, confidentiality and integrity. To further ensure the information availability, confidentiality and integrity there also exist certain rules concerning what kind of information that is legitimate to transfer via certain transfer channels.

Confidentiality is a main concern for the banks. The confidentiality agreement[4], which is valid between an employer and his employees for the rest of the employees' life, provides the banks with a fundamental security concerning information confidentiality. The banks are very strict when it comes to confidentiality since this in fact is the main selling product of every bank. The confidentiality thinking is permeated through the organisations as a whole. The confidentiality rules concerning client information is important as well as the confidentiality rules in relation to business partners of the banks.

White, (2003) emphasises the importance of traceability possibilities such as capturing and recording of all file transfers. If a bank is not able to trace different transactions it might constitute a risk and therefore traceability possibilities are well implemented in all banks systems. It is an important part of the information risk management. It makes employees aware of the monitoring possibility, which result in increased carefulness and responsibility for their actions.

In addition, information risk management is about having a risk aware culture and educating staff about the information risks (IAAC, 2003; Hussain, 2000). According to our study, all the banks put a lot of time, effort and capital into education, which has triggered a great commitment and attention for information risk management among the employees. Also the media attention to information risk has increased the awareness. Thus, the so-called, information risk culture within the organisations has improved the past years.

It is very interesting to note that when it comes to managing the information risk within the banks, they work in a very similar manner. We have not found any direct management approaches that divide them apart. Different risks have been the main focus for banks for several years and our empirical study shows that they take all risks issues very serious. They have a lot of expertise when it comes to managing risks and the expertise is obviously applied to the information risk issues as well.

[4] In Swedish, *sekretessförbindelse*

5.2.4 TRENDS

Information technology and techniques have undergone an immense change over the past decades (Bessis, 1998; Marshall, 2001) and our empirical study confirms that information risks and security is a growing concern among our interviewed banks as well. They especially emphasise that information risks can no longer be regarded only as a simple "IT-issue", which the "IT-department" has to deal with. Instead of concentrating on information technology and other technical issues, it is time to start focusing on questions such as, why protection need to be implemented, what the intentions are, and what is important for us to protect? Technical solutions are of course still necessary when it comes to secure the information, but several other parameters should be taken into consideration. The trend is moving towards a more all-embracing perspective of the information risk management, which is a result of an increased understanding of the origin of the information risks. Nordea and Danske Bank emphasise that the issue of today is not only about implementing better technical solutions to secure the information, it is as well about rules, policies and education in order to make people understand the information risk and where they derive from. Nordea further remarks that the information risk awareness should permeate the whole organisations. FöreningsSparbanken comments that company value today consists of intangible assets rather than tangible assets, which of course results in a greater focus on information risks. The banks are all well aware of that the trend that takes us more and more towards an information and knowledge society is not going to change direction; instead it is going to be more and more visible. SEB emphasises that information sources are becoming more mobile, i.e. it is not only a matter of computers anymore, also smart telephones, PDA's, etc. resulting in increased locations where information and thus information risks exists and arise.

Discussing trends with the banks we noted that it is a topic where they have a lot of visions and thoughts about the future. They all believe it is an important issue and it is essential to be on top of the development to be able to secure the information in a proper way. The risk management has to follow this trend and keep up with the development concerning information availability, integrity, confidentiality, and traceability in different contexts.

5.2.5 AWARENESS, COMMITMENT AND INVOLVEMENT

According to the theory chapter, the chief executive officer and the top management are considered to be the ultimate risk officer of the firm (Shimpi, 1999). The risk awareness and commitment should however permeate the whole organisation (IAAC, 2003; Computer Weekly, 2004). The theory states that the commitment and risk awareness is rather poor within

companies of today and that some organisations tend to ignore risk rather than plan for it and manage it (Computer Weekly, 2004).

The situation within the organisations of our empirical study show that the risk awareness and commitment to information risks, at all levels, is rather sufficient. All the banks have, as said earlier, assigned risk responsibility on Group level and the responsibility is disseminated into all levels within the organisations. This is a progress that has evolved during the last years as the banks have built their asset value on information as well as increased their need and dependence on information technology. However, it seems to exist inertia inherent in the risk awareness process, i.e. the need for information technology and information assets have been around for a longer period of time than the risk awareness. Thus, the risk and security activities have mainly increased as a result of that the knowledge and understanding of the risk related to information has improved during the last years.

The fact that the responsibility starts of, more or less, on a high level within the organisation are an indication of that the top management's commitment to information risk issues is well initiated. This is reflected in the creation of information security units within the banks. SEB is a good example of a bank that has grasped the importance of an information security unit. Their approach with a unit in the middle, working both upwards towards top management and downwards towards the business areas, results in increased awareness of information risks throughout the whole organisation. Also Nordea is a good example, where information risk "missionaries" on Group level, are assigned to build up a risk culture and in that way increase the importance of information risk awareness within the bank. FöreningsSparbanken apply about the same approach as Nordea since they have a person on Group level working to increase the awareness of information risk throughout the bank. Both Nordea and FöreningsSparbanken rely on every business area manager to carry on the risk management within their respective business area. Compared to SEB, these two banks do not have a unit in the middle supporting the procedure both ways.

However, it is also worth mentioning that although the awareness and commitment is improved on top management level, the direct involvement is not always optimal. Danske Bank mentioned for example that, in some cases, the top management still thinks in terms of technology aspects and rely on the information technology division to "build away" threats. One reason for might be the fact that it is easier to receive resources for technical, concrete solutions compared to investing in knowledge

Employees, on the other hand, who work with information and are faced with risk, on a daily basis, tend to easily grasp the importance of securing the information. All the banks state that it is quite uncomplicated to build up involvement and commitment from below. Every employee can be said to have information risk management as part of his or her work assignments. Also other stakeholders, such as clients and business partners are pushing the banks towards an improvement of its risk culture.

6 DISCUSSION & CONCLUSIONS

In this final chapter we will present the main conclusions drawn from the analysis and we will relate them to our purpose and problem definition. The section starts with a discussion regarding the underlying problem area of the study, trying to answer the main question. It is ended with answers to every sub question.

To start with we will discuss the focus of our thesis on a general basis in order to answer our main question, which was:

Investigate the concept of information risk management and how it is perceived within major banks in Sweden.

Investigating the concept of information risk management has not been an easy task, although it has been interesting. During our research we have realised that several aspects, which we assumed to be deficiencies in the beginning of the thesis are not in fact problematic in the bank environment.

In the beginning of our research we stated that the management of information risk is not well established and the solutions that are implemented are mainly focused on technology. Based on our research we claim that this viewpoint is incorrect. The banks put a lot of time, effort and money into both technical as well as organisational solutions, resulting in a holistic risk management approach. It is however important to point out that managing risk is the fundamental business concept of the banks and therefore it is not surprising that they are at the forefront when it comes to information risk management. The previously made statement implying that information risk management is not well established, have probably not been based on studies conducted on banks, which could explain the different result.

In addition, we assumed that the top management was not involved in the process of information risk management, in the same way as they are in other risk issues. We claim that this statement is incorrect as well. We draw the conclusion that they are well aware and show great commitment to information risk management. Of course, some banks have shown more commitment and involvement in the risk management process than other banks, but on an overall basis we claim that the awareness within all banks in our study is surprisingly good. We have however not compared the top management's involvement in information risk management

in relation to other risk areas. It is possible that they devote more or less time to certain risk areas, but that is a question we have not investigated.

Our sub questions give answers to more specific issues. We will below go through them one by one and comment on the results.

How is operational risk defined and what responsibility areas are included in operational risk management?

Operational risk is most commonly defined as *the risk of direct and indirect losses resulting from inadequate or failed internal processes, people and systems or from external events*. A few years ago definitions of operational risk were more ambiguous, but because of the development of new regulations, such as the Basel Capital Accord, the banks in our study follow the same approach. As a result the definition of operational risk has developed and become more precise. The banks have assigned a person to have the main responsibility for operational risk and thereby becoming the Head of Operational Risk. In those cases where information risk is considered as part of operational risk the responsibility question looks a bit different. We will discuss this further below.

How is information risk defined?

From our research we can draw the conclusion that it does not exist a definite definition of information risk. Yet, it is quite obvious what the banks consider constitute information risks. It is clear that our respondents consider information risk to include more than just technical risks. They all emphasise that information risks might be caused by other factors such as organisational structure, human errors, incorrect set rules and policies etc. To sum up, information risks are considered to be anything that might negatively affect the *availability, confidentiality, integrity* or *traceability* of information.

What responsibility areas are included in information risk management and how is the work structured?

When studying the findings from our empirical study we find that the structure of the risk work within the banks, differ to some extent. They all have an all-embracing responsibility unit, but the work assignments of these units as well as the constellation of them vary. It does not seem to exist any fundamental accepted norms concerning how to structure the work and who to appoint responsible for these issues. Every bank has an individual information risk management solution, which is almost certainly influenced by the overall organisational structure of the bank. We do not believe there are any best practices. However, common for all the banks is the main

responsibility on Group level along with the diversified responsibility among managers and employees within respective business areas.

What main risks constitute a threat to the information and how is the information secured?

As said earlier, information risks are considered to be anything that might negatively affect the availability, confidentiality, integrity or traceability of information. The risks can be caused by factors such as technical features, organisational structure, human errors, incorrect set rules and policies etc. To be able to secure the information resources are put on well-developed and complex technological solutions along with carefully developed frameworks consisting of rules and policies. Also, continuous education is an important part of information risk management.

What kinds of changes concerning information risk have been most legible during the last decade and what kind of changes are expected in the future?

According to our findings and analysis, the main trend concerning changes/development of information risks is that information risks can no longer be regarded as an IT-issue, which the IT- department has to deal with. Based on the fact that information- and knowledge society is constantly evolving, the trend is moving towards an all-embracing perspective to information risk and the management of these risks.

Investigate the extensiveness of top management's awareness and involvement regarding information risk management.

Based on our research we are able to conclude that the top management are, in most cases, well aware and have a fundamental understanding for information risks. The fact that main responsible persons exist on Group level is a good indication of top management's awareness and concern for information risk management. As a result the information risk awareness is also well permeated throughout the organisations.

6.1 FUTURE RESEARCH

In this section we will briefly address some reflections to future research within the area of information risk management.

This thesis shows how financial institutions in Sweden perceive information risk and what precautions they take to manage the risks in order to secure their information. We have only met with four banks and the conclusions drawn from this study might give an indication of how Swedish financial organisations handle this matter. However, further, more profound research based on a larger selection of organisations would of course give a more correct picture of the situations.

Further research could also be focused on developing proposals on improvements and best practices within the area of information risk management.

Financial risk managers have developed well-defined risk processes and organisational structures to measure, analyse and manage financial risk within the business. Based on this, it could also be interesting to conduct a comparable study, focusing on the possibility of applying financial risk management techniques to information risk management.

REFERENCES

LITERATURE

Alvesson, M. Deetz, S (2000). *Kritisk samhällsvetenskaplig metod,* Lund: Studentlitteratur

Alvesson, M. Sköldberg, K (1994). *Tolkning och reflektion,* Lund: Studentlitteratur

Backman, J. (1998). *Rapporter och uppsatser*, Lund: Studentlitteratur

Bessis, J (1998). *Risk Management in Banking.* Chichester: John Wiley & Sons Ltd

Brealey, R. & Myers, S. (2000). *Principles of Corporate Finance.* New York: McGraw-Hill Companies.

Eriksson L. T, Wiedersheim-Paul, F (1997). *Att forska utreda och rapportera,* Malmö: Liber Ekonomi

Holme, I., M. & Solvang, B., K. (1997). *Forskningsmetodik: om kvalitativa och kvantitativa forskningsmetoder.* Lund: Studentlitteratur.

Hussain, A. (2000). *Managing operational risk in financial markets,* Oxford: Butterworth Heinemann

Kvale, S (1997). *Den kvalitativa forskningsintervjun,* Lund: Studentlitteratur

Lekvall, P. & Wahlbin, C. (1993). *Information för marknadsföringsbeslut.* Göteborg: IHM Förlag

Marshall, C. (2001). *Measuring and Managing Operational Risks In Financial Institutions.* Singapore: John Wiley & Sons Ltd

Merriam, S., B. (1994). *Fallstudien som forskningsmetod.* Lund: Studentlitteratur.

Patel, R. & Davidsson, B. (1994). *Forskningsmetodikens grunder - Att planera, genomföra och*

rapportera en undersökning. Lund: Studentlitteratur.

Saunders, A. (2000). *Financial Institutions Management: a modern perspective.* New York: The McGraw-Hill Companies

Shimpi, P. (1999). *Integrating Corporate Risk Management.* New York: Texere LLC

Thurén, L. (1996). *Vetenskapsteori för nybörjare.* Stockholm: Liber

Wallén, G (1996). *Vetenskapsteori och forskningsmetodik,* Lund: Studentlitteratur

Waring, A. & Glendon A., I. (1998). *Managing risk,* Hong Kong: International Thomson Business Press

Yin, R., K. (1994). *Case study research: design and methods.* Thousand Oaks, California: Sage Publications, cop.

ARTICLES

Baker, S., Ponniah, D. & Smith, S. (1998). Techniques for the Analysis of Risk in Major Projects, *The Journal of the Operational Research Society,* Vol. 49, No. 6, 567-572.

Blake, I. & Sirkka, L., J. (1991). Applications of Global Information Technology: Key Issues for Management, *MIS Quarterly,* Vol. 15, No. 1, 33-49

Bowling, D., J. & Fredrick, R., L. (2003). Taking the Enterprise Risk-Management Journey. *Aspen Publishers Inc.*, Feb, Vol. 16, No. 2.

Cassidy, S. Constand, R. Corbett, R. (1990). The Corporate Value of the Corporate Risk Management Function, *The Journal of Risk and Insurance,* Vol. 57, No. 4, 664-670

Close, D., B. (1974). An Organization Behavior Approach to Risk Management, *The Journal of Risk and Insurance,* Vol. 41, No. 3, 435-450.

Gordon, L. Loeb, M (2002). The Economics of Information Security Investments, *ACM Transactions on Information and System Security,* Vol. 5, No. 4.

Gupta, M., Chaturvedi, A., Mehta, S., Valeri, L (2001). The Experimental Analysis of Information Security Management *Issues for Online Financial Services.* Krannert Graduate School of Management Purdue University U.S.A., International Center for Security Analysis, King's College, London, United Kingdom.

Kotulic, A., G. & Clark, J., G. (2004). Why there aren't more information security research studies, *Information & Management,* Vol. 41 No. 5

Macklin, B., De Tora, D., Rath, E. & Rothman, P. (2003). A Partnership Approach to Operational Risk Management, *Bank Accounting & Finance (Aspen Publishers Inc.)* Vol. 16, No. 6.

Marshall, J. & Heffes, E., M. (2003). Study Faults Bank Risk Management, *Financial Executive,* Vol. 19, No. 9.

Pardas, A. (2002). What matters for effective information security, *New Straits Times-Management Times (Malaysia).*

White, K. (2003). Risk Averse, *Computer Business Review*, Vol. 11, No. 3

Xystros, C. & Weber, R., E. (2001). Information risk management, *Traffic World,* Vol. 265, No. 13.

PRESS

Business chiefs look for workable IT policies, Computer Weekly, 02-27-2004

Establishing a Solid Security Foundation, eWeek, 03-15-2004, Vol. 21 No. 11

Lövgren, P. (2004). *Riskanalys kan rädda hela verksamheten*, MikroDatorn no 3.

SAS Survey Shows Companies Hit by Operational Risk, Computergram Weekly, 09-10-2003 No. 4752

INTERNET

Bank for International Settlements,
www.bis.org

Danske Bank,
www.danskebank.com

FöreningsSparbanken,
www.foreningssparbanken.se

Information Assurance Advisory Council, IAAC,
www.iaac.org.uk

IAAC (2002), *Engaging the Board: Corporate Governance and Information Risk,*
http://www.iaac.org.uk/Initiatives/CG%20Recommendations%20Paper.pdf

KPMG,
www.kpmg.com

KPMG, (2002). *Information Security Survey*,
www.kpmg.com/microsite/informationsecurity/isssurvey.html

Nordea,
www.nordea.com

O'Brien, N., Smith, B. & Allen, M. (1999). *The case for quantification*,
FinanceWise,
www.financewise.com/public/edit/riskm/oprisk/opr-models.htm

Rathmell, A. (2002). *Corporate Governance and Information Risk Management,*
http://www.it-analysis.com

SEB,
www.seb.se

Swedish Standard Institute,
www.sis.se

The information cycle
http://appling.kent.edu/ResourcePages/LTStandards/Chart/infocycle.html

Writing@CSU (2004-05-22). *Reliability*,
http://writing.colostate.edu/references/research/relval/pop2a.cfm

Östgöta Enskilda Bank, www.oeb.se

INTERVIEW RESPONDENTS

Carlén, Tobias, Information Risk Management Specialist, KPMG, 2004-03-10, 2004-04-28

Gee, Kathryn, Specialist Group Security, FöreningsSparbanken, 2004-05-06

Holmsten, Kjell, MB IT Strategy Information Security, SEB Merchant Banking, 2004-05-07

Hummel, Tobias, Operational Risk Control, SEB Merchant Banking, 2004-05-07

Högberg, David, MB IT Strategy Information Security, SEB Merchant Banking, 2004-05-07

Palmén, Erik, Head of Group Operational Risk Management, Nordea, 2004-04-29

Peterson, Hans, E., Vice President - Security, Danske Bank, 2004-04-29

Sefastsson, Lars, Head of Group Operational Risk, FöreningsSparbanken, 2004-05-06

APPENDIX 1

INTERVIEW QUESTIONS

Operational risk management

Definition

1. Hur skulle du kortfattat definiera ”Operational risk”?
2. Vilka områden ligger under ”Operational risk”?
    2.1. Kan Du rangordna dessa områden?

Ansvar

3. Är det du som har det övergripande ansvaret för operationella risker på din bank?
    3.1. Om ja, vad är din titel?
    3.2. Om inte, vem har ansvaret och vad är hans titel?
4. Finns det flera ansvariga indelat på delområden inom operationell risk?
    4.1. Om ja, hur är de indelade?
    4.2. Om nej, varför inte då?
5. Vad är din huvuduppgift? (vad lägger du mest tid på?)

Information risk management

Definition

6. Hur skulle du definiera begreppet information risk management?
7. Vilka områden anser du att begreppet information risk management täcker?
8. Information risk management skulle kunna definieras som något av följande, vilket anser du stämmer bäst överens med er bild av konceptet?

”att information risk management är en teknisk supportfunktion med fokusering på hårdvara och mjukvara”

eller

”att information risk management är en affärskritisk operationell funktion som fokuserar mer övergripande på tillgänglighet, integritet, riktighet och sekretess av informationen”

Organisation, struktur och ansvar

9. Har ni någon informationsrisk avdelning?
    9.1. Om ja, vad kallas den för specifikt?
        9.1.1. Vad gör den avdelningen? (om en källa till risk upptäcks vilka åtgärder tas?)
        9.1.2. Vad lägger den avdelningen mest tid på? (vilket område?)

9.1.1. Faller avdelningen för informationsrisker inom ramen för avdelningen för operationella risker?

9.1.1.1 Om ja, hur stor är avdelningen för informationsrisker inom avdelningen för operationella risker?

9.1.1.2. Om nej, varför faller avdelningen för information risker inte inom avdelningen för operationella risker?

9.1.2. Vem är ansvarig för avdelningen för informationsrisker?

9.1.3 Hur många personer arbetar inom detta området?

9.2. Om nej, varför inte, vad faller frågor rörande detta under för avdelning istället? (IT-avdelningen, avdelning för operationella risker, annat)

Trender

10. Hur har risker inom information risk management förändrats/utvecklats de senaste årtionden fram till idag? (risker relaterade till er Internetbank och dess ökade användning, risk nu och då)

10.1 Varför tror du att förändring har skett?

10.2 Hur tror du att det kommer att förändrats/utvecklats i framtiden?

Informationsrisker och hot

11. Vilka risker anser du hotar informationen inom banken?

12. Kan du rangordna följande risker?

Läckage av information?

Tillgänglighet till information?

Modifiering av information på fel sätt?

Spårbarhet?

Andra risker och hot?

Läckage

13.1. Vad har ni för regler uppsatta med avseende på relationer med affärspartners? (är det några kontrakt, andra former av avtal)

13.2. Om en anställd säger upp sig, på vilket sätt kan den företagskänsliga information som han har skyddas? (sekretessavtal, karantäner etc.)

13.3. Vilka riktlinjer finns det för den dagliga kommunikationen internt samt extern för företaget? (skicka information via e-mail, instant messenging odyl)

13.4. Hur hindrar ni anställda att inte ta med sig information hem som de inte egentligen ska ta hem? (kundregister, info rörande andra avd.)

Tillgänglighet

14.1. Vilka rutiner och policies har ni för att gardera tillgängligheten av information (t.ex. om en nyckelperson är sjuk eller försvinner eller dennes dator exploderar)?

Modifiering/riktighet

15.1. Vad har ni för policies och regler för vem som får göra vad med viss information, med andra ord, vad har ni för regler för vem har access och vem som inte har?

15.2. Vad har ni för skydd för externa attacker?(brandväggar odyl)

Spårbarhet

16.1 Hur kan ni spåra vem som har gjort vad vid vilken tidpunkt med viss information? (banktransaktioner, modifieringar i filer, e-mail)

Förebyggande åtgärder

17. Hur fördelas resurserna på de olika delarna inom information risk management? (hur fördelas resurser på tex. tekniska lösningar, utbildning, strategisk planläggning etc.)

17.1. Om mest resurser fördelas på tekniska lösningar, anser du att skyddandet av information kan bestå av mer än endast tekniska lösningar?

18. Hur medvetna anser du att de anställda i din organisation är om informationsrisker? (Riskmedvetenhet, riskkultur)

19. Utbildas personalen i säkerhets och riskfrågor kontinuerligt

19.1. Om ja, hur och i vad utbildas de?

19.2 Om nej, varför inte?

20. Hur kontrollerar ni att policies följs och att de får genomslagskraft?

20.1 Hur pass realistiska anser du att reglerna är? (för hårt dragna?)

Ledningens engagemang och involvering

21. Hur involverad och engagerad är toppledningen i frågor rörande information risk management?

22. Kommer direkta strategiska direktiv från toppledningen eller ligger det strategiska ansvaret på annan nivå?

APPENDIX 2

BRIEF HISTORY AND FACTS ABOUT SEB

André Oscar Wallenberg founded Stockholms Enskilda Bank in 1856, as Stockholm's first private bank. In 1915, SEB moved its head office to Kungsträdgårdsgatan. During the 1960's and 1970's SEB became the bank for industry to a greater extent. The aim was to create a bank, which could meet the competition from the major international banks. Today, the SEB Group is a North European financial banking group for companies, institutions and private individuals. Although its main activities consist of banking services SEB also conducts important life insurance operations both within and outside Sweden. SEB has a total of 670 branch offices around Sweden, Germany and the Baltic States and more than four million customers, of whom 1.6 million are e-banking customers. On 31 December 2003, the Group's total assets amounted to SEK 1,279bn, while its assets under management totalled SEK 822bn. The Group is represented in some 20 countries around the world and has a staff of about 18,000. Merchant Banking is a part of SEB, which supplies financial services and products to major Nordic corporate and financial institutions. One important goal for the Merchant Bank is to meet the customers at an early stage of their internal and external financial processes, which often result in long-term relationships with the customers. Around 2,000 people work at Merchant Banking, which operates in 12 countries. (www.seb.se)

APPENDIX 3

BRIEF HISTORY AND FACTS ABOUT NORDEA

Nordea originate from four Nordic banks: Merita Bank, Nordbanken, Unibank, and Christiania Bank and Kreditkasse, from Finland, Sweden, Denmark and Norway respectively. Since December 2001 all operations have been conducted under the brand name of Nordea. The bank today is the largest financial services group in the Nordic and Baltic Sea region The bank has been at the forefront of developments and today it is a player in the region who has made the a significant progress in terms of the integration of banking and insurance activities across national boundaries. The bank has come a long way towards being recognised as the leading provider of financial services in the Nordic and Baltic Sea region. The Group's business organisation includes three business areas: Retail Banking, Corporate and Institutional Banking, and Asset Management & Life. Each business area is responsible for financial results, customer relations, distribution, products and business development and support. Nordea has a large customer base of any financial services group in the region, including 9.6 million personal customers, 900,000 corporate customers and 1000 large corporate customers. The bank also has a comprehensive distribution network in the region including 1,224 bank branch offices and leading telephone banking and Internet services. Group's total assets amounted to approximately EUR 262bn in 2003. (www.nordea.com)

APPENDIX 4

BRIEF HISTORY AND FACTS ABOUT FÖRENINGSSPARBANKEN

FöreningsSparbanken was founded in 1997, by the merger of Föreningsbanken and Sparbanken Sverige. The bank's composite history dates all the way back to 1820, when Sweden's first savings bank was founded, in Gothenburg. At the turn of the year 2003-2004, FöreningsSparbanken had approximately 15,400 employees, of which 9,500 in Sweden. The group has about 4.3 million private customers in Sweden and four million in the Baltic States. Independent savings banks and partly owned banks have an additional 1.7 million private customers. As of 31 December 2003, FöreningsSparbanken had a balance sheet total of SEK 1 002 billion, deposits of 275 billion and lendings totalling 826,4 billion. Operating profit for the year 2003 was SEK 9 564 million; return on equity: 15,9%. The business concept of the bank is to be the obvious choice among banking alternatives for private individuals, companies, the agricultural sector, municipalities, county councils and organisations by offering a range of customised easy-to-use financial services. FöreningsSparbanken positions itself as a market leader when it comes to household savings, fund savings and various kinds of individual pension savings schemes. The bank's share of the corporate market is 20-30% when it comes to deposits, lending, leasing and financing. (www.foreningssparbanken.se)

APPENDIX 5

BRIEF HISTORY AND FACTS ABOUT DANSKE BANK

Östgöta Enskilda Bank was founded in February 24, 1837 with its head office in Linköping. The bank is a strong believer in local bank office presences and therefore province banks are established in city after city. In 1997 Danske Bank acquired the different province banks. In 1997, Danske Bank acquired the different province banks, which turned Östgöta Enskilda Bank into an international bank. In 2004 the location of the head office is moved from Linköping to Stockholm. The bank still operates emphasising, "All business is local". The bank offers its services to both the private market and to the largest international organisations. The Danske Bank Group is a diversified financial services company providing a wide range of services to some 3 million retail customers and 150,000 corporate customers, primarily in Denmark and northern Europe. The Bank's customers in Denmark have access to an extensive branch network, several corporate banking centres, various subsidiaries and the head office in Copenhagen. The 46 branches of Östgöta Enskilda Bank and Corporate Banking, Stockholm, as well as head office departments serve Swedish customers. Around 1200 people work at Östgöta Enskilda Bank (Danske Bank) in Sweden (www.oeb.se; www.danskebank.com).

APPENDIX 6

BRIEF FACTS ABOUT BASEL II

The Basel Committee, established by the central bank Governors of the Group of Ten countries at the end of 1974, meets regularly four times a year. It has about thirty technical working groups and task forces, which also meet regularly. The Committee's members come from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, United Kingdom and United States. Countries are represented by their central bank and also by the authority with formal responsibility for the prudential supervision of banking business where this is not the central bank.

The Committee does not possess any formal supranational supervisory authority, and its conclusions do not, and were never intended to, have legal force. Rather, it formulates broad supervisory standards and guidelines and recommends statements of best practice in the expectation that individual authorities will take steps to implement them through detailed arrangements - statutory or otherwise - which are best suited to their own national systems. In this way, the Committee encourages convergence towards common approaches and common standards without attempting detailed harmonisation of member countries' supervisory techniques.

In 1988, the Committee decided to introduce a capital measurement system commonly referred to as the Basel Capital Accord, commonly known as Basel I. This system provided for the implementation of a credit risk measurement framework with a minimum capital standard of 8% by end-1992. Since 1988, this framework has been progressively introduced not only in member countries but also in virtually all other countries with active international banks. In June 1999, the Committee issued a proposal for a New Capital Adequacy Framework to replace the 1988 Accord, commonly called Basel II. The proposed capital framework consists of three pillars: minimum capital requirements, which seek to refine the standardised rules set forth in the 1988 Accord; supervisory review of an institution's internal assessment process and capital adequacy; and effective use of disclosure to strengthen market discipline as a complement to supervisory efforts. Following extensive interaction with banks and industry groups, a final consultative document, taking into account comments and incorporating further work performed by the Committee, was issued in April 2003, with a view to introducing the new framework at end-2006.

APPENDIX 6

The Committee believes that operational risk is an important risk facing banks and that banks need to hold capital to protect against losses from it. Within the Basel II framework, operational risk is defined as the risk of losses resulting from inadequate or failed internal processes, people and systems, or external events. This is another area where the Committee has developed a new regulatory capital approach. As with credit risk, the Committee builds on banks' rapidly developing internal assessment techniques and seeks to provide incentives for banks to improve upon those techniques, and more broadly, their management of operational risk over time.

The Basel Committee has proposed four approaches for calculating operational risk. Financial institutions may select from this menu the approach which is most suitable for their form of business and which they can apply most effectively. As will be seen they vary in complexity.
The four methods of calculation are:

The Basic Indicator Approach**,** based on a percentage of gross income

The Standardised Approach**,** which calculates a separate operational risk charge for each line of business, based, primarily, on the size of that business

The Internal Measurement**,** which allows institutions to apply a calculation, prescribed by The Basel Capital Accord to internal loss data

The Loss Distribution Approach**,** this is the most sophisticated approach, which the Basel Committee has yet to spell out in detail.

(www.bis.org)