UNIVERSITY OF VAASA

FACULTY OF BUSINESS STUDIES

FINANCE

Jussi Jalasto

OPERATIONAL RISK MANAGEMENT IN FINNISH INSURANCE COMPANIES (CASE: COMPANY X)

Master's Thesis in Accounting and Finance

Finance

VAASA 2016

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

UNIVERSITY OF VAASA
Faculty of Business Studies
Author: Jussi Jalasto
Topic of the Thesis: Operational Risk Management in Finnish Insurance Companies (Case: Company X)
Name of the Supervisor: Professor Vanja Piljak
Degree: Master of Science in Economics and Business Administration
Department: Department of Accounting and Finance
Master's Programme: Finance
Year of Entering the University: 2009
Year of Completing the Thesis: 2016 **Pages:** 99

ABSTRACT

Operational risk management is one of the broadest functions of any financial institution and one of the hardest to control. It is also a rather new risk category; companies around the world are paying more and more attention to operational risks. Financial institutions and researchers have realized that it is essential to try to identify all risks, not only market, credit and strategic, but also operational risks.

The aim of this study is to investigate the existence of operational risks in Finnish insurance companies, especially Company X, and clarify the key operational risks. In terms of operational risk and operational risk management Finnish insurance companies are on the borders of transition. It is important to analyze the current stage of operational risk management so that further development could take place in the future.

The data in this qualitative research has been collected from interviews with operational risk managers working at insurance companies in Finland and from the employees of Company X. Operational risk managers from Finnish insurance companies offer a broad and professional perspective to the questions while employees from Company X bring a more detailed and pragmatic approach to the answers. Interviewees responded to a questionnaire that was sent to them before face-to-face interviews.

The results show that Finnish insurance companies are very aware of operational risks, but the tools used are still relatively simple. Systems-related risks, human risks, technological development and regulations are the four main operational risks that Finnish insurance companies face today. There is one clear similarity between the tools and methods used by insurance companies in Finland and it is also the tool used to prioritize resources for operational risk management. The results provide evidence that operational risk management in Finnish insurance companies needs further and more specific research so that companies could improve their own operational risk management.

KEYWORDS: Operational risk, insurance company, regulations, system

1. INTRODUCTION

Operational risk management is one of the broadest functions of any financial institution and one of the hardest to control. Operational risks are also very hard to categorize. If we go back to the 1980s operational risk management did not even exist, but in the past two decades knowledge of operational risk has grown rapidly. Esterhuysen, Vuure and Styger (2010) say that operational risk is not a new concept for banks although the collection and evaluation of data for operational risk only dates back two to three years (six to seven years from 2014). Financial institutions and researchers have realized that it is very important to try to identify all risks, not only market, credit and strategic but also operational risks. After identifying all the risks managers must decide how to use limited resources to prioritize and manage these risks. Studies have also shown how challenging it is to collect data for operational risk management since there is only limited data available; this in turn highlights the importance of the correct interpretation of the data.

Operational risks manifest themselves in numerous ways, for example: internal or external fraud, rogue trading, terrorism, environmental hazards, systems breakdown or even sabotage. Operational risks also include human risk, legal risk, information risk and reputational risk. All these operational risks need to be managed in different ways. Controlling or predicting these kinds of risks is obviously quite challenging. It is also difficult to agree on an exact definition of operational risk because its broadness. Basel 2 defined operational risk as follows: “the risk of direct or indirect loss resulting from inadequate or failed internal processes, people or systems or from external events”. (Basel Committee on Banking Supervision 2001). This definition includes legal risk but excludes strategic and reputational risk. Companies have generally accepted this definition as the standard.

The aim of this study is to investigate the existence of operational risks in insurance companies (Company X) and clarify what those risks are. Although managing operational risks is similar across the whole in the financial sector, little attention has been paid to the retail banking and investment banking areas. The target is also to assist insurance companies to recognize their key operational risks in Finland. Finally it is intended to create a theoretical framework that can be used to support (Company X’s) internal/external operational risk management.

1.1 Research question

This research is focused on operational risk within Finnish insurance companies, especially the Company X. The main point of the study is to identify the key operational risks, particularly those that have the largest impact on Company X's everyday processes. Once the key operational risks are identified, the main focus is to offer solutions using some of the most common tools for operational risk management. These tools can be found in operational risk management work in Finnish insurance companies and research on operational risk management. The research questions are:

- What are the key operational risks in the Finnish insurance company (Company X)?
- What are the most common tools used in operational risk management?
- How to prioritize and allocate resources between different operational risks?

When the key operational risk and the tools have been found it is important to know where and how to prioritize and allocate the limited resources of the company.

1.2 Structure of the study

The structure of the study is quite simple. After the introduction I will start by opening up the meaning of basic business risks, in particular credit, market, strategic, and finally operational risk. I will use both previous research on the topic and relatively new publications. This second chapter of my study should inform the reader of the basics of business risk management in the financial sector. I will also give some practical examples of operational risk and the most up to date methods to measure it. Although this study focuses on operational risk in the insurance business, I have included a lot of information from Basel 2 regulations for operational risk. This is because banks and insurance companies have a rather similar perspective on operational risk management.

In the third chapter the focus is on operational risk. This chapter will provide a more advanced view of operational risks and operational risk management.

In the fourth chapter I will concentrate on the operational risk management in insurance companies. Firstly, I will provide a more global view of operational risk management in insurance companies then move on to a more domestic perspective as some risks, such as environmental and legal, are different in Finland than in the rest of the world. It is

necessary to identify regional differences and similarities but, of course, these boundaries are shrinking all the time thanks to the European Union and rapidly advancing globalization. This section will also be based on previous literature and research, however, following the comparison of global and domestic viewpoints, I will start the research part of this study.

In my research I will identify the key operational risks in the Finnish insurance company/ Company X. Here the reader should understand the separation between key operational risks and less significant operational risks. It is also important to find out which are the most common tools used in operational risk management and how to resources allocated to operational risk management are prioritized between different operational risks. At this point I will carry out qualitative research into operational risks using a questionnaire and existing publications.

Finally, I will create a helpful, indicative guide for Company X's operational risk management based on the results of the investigation carried out in the study and then reveal my conclusions.

2. BUSINESS RISKS

2.1 Overview on the basics of business risks

Nowadays there is a seemingly infinite number of risks that surround the business world and companies operating in it. Risk Management has become a vitally important factor as a result of globalization and the continuing demand for greater returns. (Clarke & Varma, 1999) It is very important to know how to prioritize your limited resources and allocate them to the right risks in order to maximize the benefits of risk management. When this is done well it provides savings to the company and thereby an advantage over its competitors.

Competition in financial markets has grown rapidly in just a few decades, therefore the management of a company has become more intensive and detailed. This development has led to companies having multiple management fields, including risk management. Increasing amounts of resources are being invested in this field. Risk management itself can be divided further into sub-sectors, the number of which varies between companies. The Basel committee of banking supervision has divided risks into three main sub-sectors: credit risk, market risk and operational risk. However, in this chapter there is one more sector in addition to those mentioned above: strategic risk. I will go through the following risk categories:

- Credit risk
- Market risk
- Strategic Risk
- **Operational risk**

Too often management focuses their concentration only on the negative consequences of the risk. (Clarke & Varma, 1999)

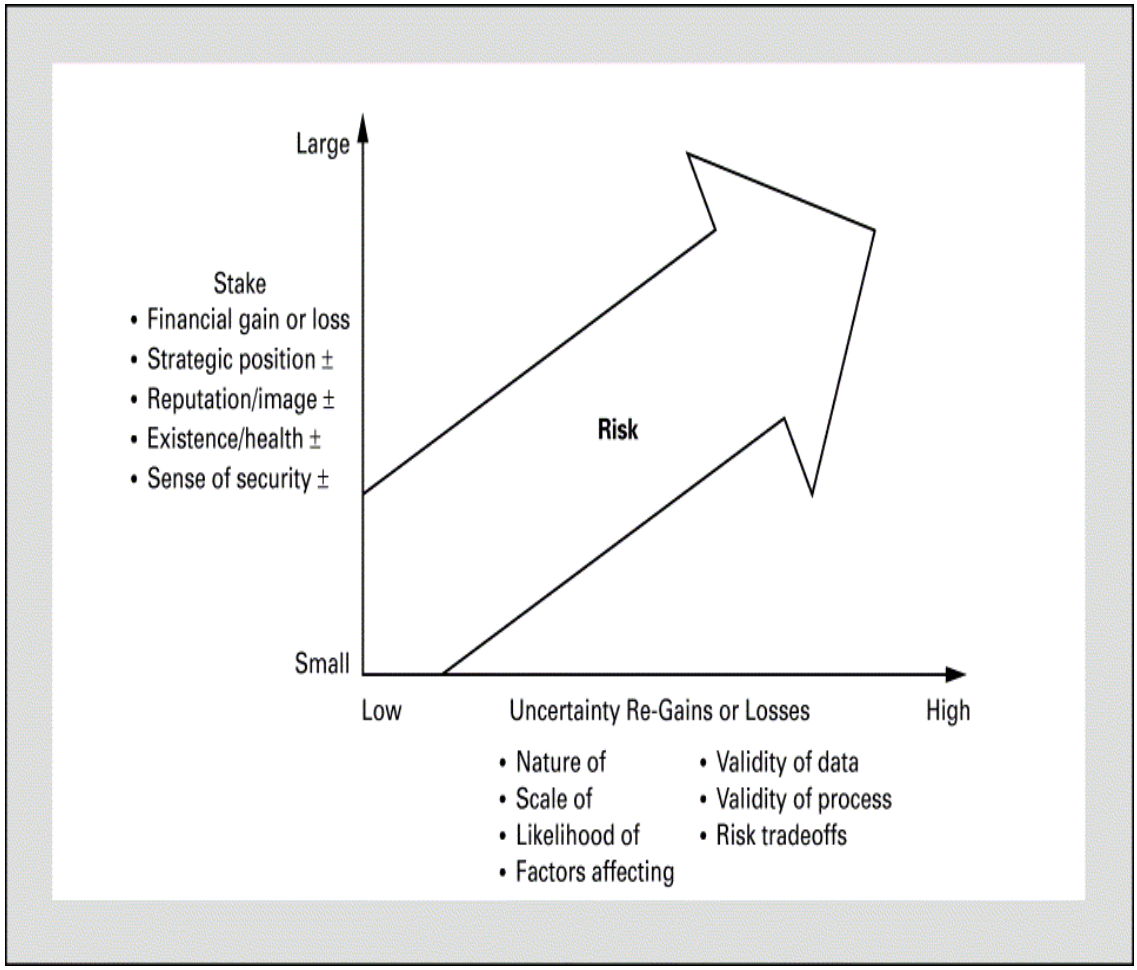

Figure 1. RISK (Clarke & Varma, 1999)

2.1.1 Credit Risk & Market Risk

Traditionally credit risk has been part of an interaction between two individual operators. When the loan was made to the borrower the credit risk remained on the lender's balance sheet until the debt was repaid or written off. In all simplicity the credit risk is the risk that borrower cannot repay the debt. However, nowadays credit risk is much more complex than before. The loan can be packaged and traded and then repackaged again. A short time ago banks and insurance companies were the only parties to offer loans. Today rating agencies, financial guarantors, and a variety of special-purpose companies, all serve as critical links in the credit chain. (Cacouette, Altman & Narayanan, 1998)

Duffie and Singleton state, “Credit risk is the risk of default or reductions in market value caused by changes in the credit quality of issuers or counterparties”. This means that today, financial markets are full of financial components under the responsibility of many participants in the market. Lopez and Saidenberg have a similar way of defining credit risk: “Credit risk is defined as the degree of value fluctuations in debt instruments and derivatives due to changes in the underlying credit quality of borrowers and counterparties.” Bonds, swaps, derivatives and other financial instruments all have more than one responsibility carrier due to the very complex structure of the financial markets. (Duffie & Singleton, 2003).

Past economic theory tells us that credit and market risk are tightly related. Not only do they have strong relationship, but they are also “not separable”. This means that if one changes unexpectedly the other changes too. When the probability of default unexpectedly changes, it generates credit risk and this affects the market value of the company generating market risk. Because these risks are related to each other similar components affect them both. Economic fluctuations have an indirect impact on credit risk but a direct impact on market risk, in fact, market risk is shaped by the uncertainty of the markets. As the name suggests, market risk results from the overall performance of the financial markets, it is also called systematic risk or “un-diversifiable risk” because it is impossible to reduce through diversification. For these reasons, it is very difficult to try to avoid market risk. (Jarrow & Turnbull, 2000).

Raghavan defines market risk as the possibility of loss to a firm caused by changes in the market variables, that is the risk that movements in equity and interest rate markets, currency exchange rates and commodity prices will affect the value of a firm. Under market risk there are more specific sub-scenes. First is liquidity risk. Liquidity is the ability to turn your assets into a more “mobilized” form, for example cash is very liquid but a company’s know-how is far from liquid. Usually the more liquid the assets are, the lower the profit. Cash in your pocket does not increase wealth. The opposite can also be true when there is a lack of liquidity to take advantage of profitable business opportunities. Balancing opportunities and increasing capital adequacy is hard work especially for banks and insurance companies

Interest rate risk is one part of market risk. Interest rate risk is the potential negative impact of the movement in interest rates. Changes in interest rates affect earnings, the value of assets and cash flow. Additionally there is currency risk and foreign exchange risk, both resulting from negative exchange rate movements. Lastly, under the market

risk, is country risk. As you can imagine there are many risks present in cross border transactions. There is the possibility that a country will be unable to repay debts to foreign lenders on time, political risk when government is taking over the assets of the financial entity (like nationalization) and of course huge cultural differences between countries can pose a risk in a specific course of action. (Raghavan, 2003)

2.1.2 Managing Credit and Market Risks

Now when we have basic idea of what these risks are, it is natural to move to management of these risks. Risk management is vital for all participants in the financial sector and the survival of a firm depends heavily on its capability to prepare for change in the future rather than just react when change is already happening. Risk management is not expected to prevent the risks facing a company, but to ensure that the company is familiar with the risks they are taking. Through comprehensive knowledge of risks it is much easier for a company to measure the risks and prepare protection plans. However these risk protection actions cost money and balancing between risk and return is not an easy task. (Raghavan, 2003) So the question remains: "Which risk protection actions should we focus on and which not".

Although the economics of risk management for financial companies is far from an exact science, it can, to a certain degree, be managed. (Duffie & Singleton, 2003) The basic idea of managing credit and market risk is try to protect the company from a loss. This loss protection applies to almost every risk category. When dealing with credit and market risk, companies have to protect themselves by managing expected loss. Expected loss is part of probability theory and the attribute expected always refers to the future. Companies have to try to "guess" their future losses, so they can prepare. These "guesses" are made with complex financial models. Credit and market risk measurement models generate forecasts of losses based on different variables. These measurements clearly have the potential to improve risk management efficiency. When the forecasted loss measurements have been carried out properly, management has a much easier job to decide how best to manage the risks. (Lopez & Saidenberg, 2000)

2.1.3 Strategic Risk

Strategic risk differs slightly from credit and market risk. When risk management works with strategic risk the question posed is, "Is there a need for change?" The world is

constantly changing and those organizations that can follow the change are in a strong position. In contrast, those organizations that cannot adapt to changes effectively enough are likely to perish. Strategic risk management makes an evaluation of the market conditions today and then makes a forecast of potential changes that will occur over a period of time. (Roberts, Wallace &McClure, 2003) Risk management can ask, "Which way is the market going in the future?" Of course, this is a question that everybody wants to know the answer to. However, for example, a decade ago post office strategic risk management might have asked, "Should we focus on traditional mailing or should we focus on mailing via the Internet?" Today it is easy to answer to that question but a decade ago it was not possible to know. These kinds of strategic decisions are vital to an organization's future.

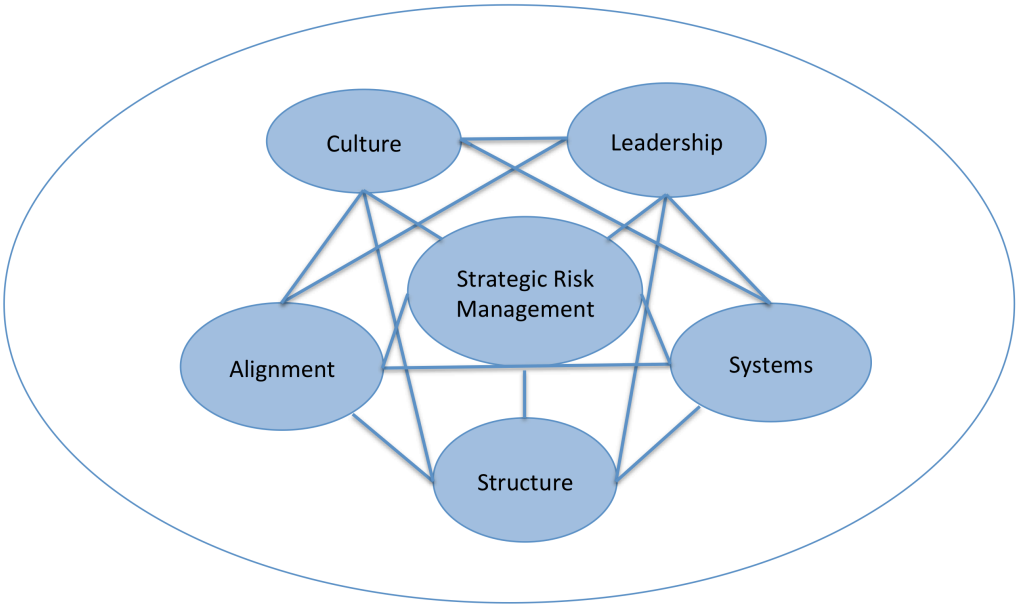

Figure 2. Strategic risk management

Strategic risk management and corporate governance often go hand in hand. Indeed, corporate governance is about making strategic decisions. Stephen A. Drev, Patricia C. Kelley & Terry Kendrick have divided strategic risks into five elements: Culture, Leadership, Alignment, System, and Structure (CLASS). Each of these five elements relates to the others. Organizational culture consists of leadership practices, systems support organizational structure and have an effect on its culture. No element stands

alone. Boards have to know that making changes in one element has an effect on the others. Poor strategic risk management can quickly remove competitive advantage.

Table 1. Risks

	Definition	Caused by	Managing
Credit risk	-Credit risk is the risk of default or reductions in market value	-Changes in the credit quality of issuers or counterparties	-Having full knowledge of the risks that the firm is taking
Market risk	-The possibility of loss to a firm caused by the changes in the market variables	-Movements in equity and interest rate markets, currency exchange rates and commodity prices will affect the value of a firm	-Having full knowledge of the risks that the firm is taking
Strategic risk	-Risk resulting from an incorrect forecast of future market trends when developing initial strategy	- Senior level misjudgments and mismanagement of risk	-Having full knowledge of the risks that the firm is taking

2.2 Operational Risk

Not all risks faced by financial institutes are in the readily categorized and modeled categories above. For example the risks of internal fraud or system breakdown do not bend easily to modeling. These kinds of risks are usually categorized in a section called operational risk. (Lopez, 2002) In the past decade, operational risk has risen from non-recognition to become a crucial factor for corporate risk management units and has played a significant role in a number of corporate collapses. No wonder it has risen so quickly straight to the core of risk management. Operational risk has generated a sizeable quantity of research and investigation in the past years. (Moosa, 2007) This chapter will open up the topic of operational risk.

2.2.1 What is Operational Risk

Operational risk has gained increasing visibility and notoriety due to past events. The media and regulators alongside business executives and corporate collapses caused by failed operational risk controls have contributed to a growing focus on operational risk. (Moosa, 2007) Although the risks of fraud, natural disaster or reputational damage have existed for centuries, the potential of operational risk made a breakthrough only recently. (Buchelt & Unteregger, 2004) Reasons for this breakthrough can be explained by technological development, increasing competition and globalization. Technological dependence, for instance, exposes a firm to system failure and therefore management has to pay closer and more serious attention to operational risk.

Regulators such as Basel 2 by the Basel Committee on Banking Supervision and Solvency 2 have defined operational risk as follow: “the risk arising from inadequate or failed internal processes, people or systems or from external events”. (Basel committee on banking supervision, 2001) and “the risk of loss arising from inadequate or failed internal processes, personnel or systems, or from external events”. (Solvency 2, Directive 2009/138/EC). These definitions are important when building regulations for financial institutions. Regulations set out the operational risks that a financial institution has to manage. Regulations are made to protect investors, clients and corporations themselves and also exist to make sure that everybody in the industry is playing by the same rules. Despite this, there are multiple arguments against regulations. Danielsson et al. 2004 uncovered some shocking side effects of setting value-at-risk constraints in an

economy. They say, “The effect of such constraints is to induce behavior that exacerbates the shocks further.” Also Kaufman and Scott (2000) concluded that many bank regulatory actions have been double-edged, if not counterproductive.

The definition published by Basel 2 is actually partly from the definition of Robert Morris Associates et al. (1999). He defined operational risk as “the direct or indirect loss resulting from inadequate or failed internal processes, people and systems, or from external events”. The Basel Committee dropped the indirect loss from the definition. In this definition reputational risk is surprisingly ignored given that reputational risk and reputational damage are very powerful factors. Although the Basel 2 definition for operational risk is said to be “official”, it has not been accepted without discussion. Turing (2003) claims that the definition of Basel 2 is “so broad as to be totally unhelpful”. Herring (2002) criticizes the definition direct from the first version where the Basel Committee started using a definition for operational risk which included all risk that is neither credit risk nor market risk. When the Basel 2 definition was narrowed to its final version, basic business risk was completely omitted. Herring’s opinion was that final definition is too narrow. Hadjiemmanuil (2003) claimed that the Committee’s definition for operational risk is “deeply flawed and it is not based on some generally accepted understanding of operational risk”.

However Basel 2 was not the only party to define operational risk. Vinella & Jin (2005) defined it as, “the risk that the operation will fail on or more operational performance targets, where the operation can be people, technology, processes, information and the infrastructure supporting business activities”. Nevertheless these definitions are just words and for risk management it should not make a big difference which words are used to define operational risk.

2.2.2 Practical Examples on Operational Risk

In this chapter we move from defining operational risk to practical observations from the financial business world. As previously mentioned, there have been corporate collapses and bankruptcies caused by realized operational risks. This chapter introduces the reader to operational risk types and some major incidents concerning operational risks.

Alexander Cambell (2012) made a list of the top 10 operational risks for 2013. The list includes all kinds of operational risk types from natural disaster to political intervention. These operational risks will give the reader a more practical understanding of what is meant by operational risk.

Top 10 operational risks for 2013:
(Alexander Campbell, Operational Risk & Regulation 2012)

Table 2. Top 10 operational risks 2013

Operational Risk	Example
1. It sabotage	- Cyber attacks
2. Reputational damage	- Banks and financial institutes least trusted sector of business
3. Incentives and compensations	- ”Mis-sold” products
4. Fraud and customer data abuse	- Economic downturn → Employees might have financial pressure → Generate frauds
5. Epidemic disease	- Severe acute respiratory syndrome 2003 (SARS) - H1N1 2009-2010
6. Political Intervention	- One of the largest potential sources of operational risk - Eurozone debt crisis ”far from over”
7. Sanctions and AML compliance	- Banks in the spotlight accused of negligently or willfully breaking anti-money laundering (AML) rules or international economic sanctions.
8. Emerging markets operating risks	- "Proper securities regulation in today's emerging markets is tantamount to "proper" regulation of tomorrow's developed markets. Therefore, emerging markets within Iosco and the global financial system are much more important than they were in the past.”
9. Business continuity and disaster recovery	- Hurricane Sandy 2012
10. Failure to enforce internal controls	- 2010 UK –bribery act - UBS roguetrader Kwelu Adoboli

All of the risks listed above are quite broad, but when realized can cause major damage. In this case Cambell focuses on low frequency high impact operational risk but actually discussion in financial studies argues for a financial corporate focus on low frequency high impact rather than high frequency low impact risks. The impact here is on capital

adequacy. Alexander Carol (2000) argues that it is more important to focus on low frequency high impact risk; regulators in particular should target their regulation on high impact risk. He did not completely dismiss high frequency low impact risks because of the "tail" loss. Tail loss is the effect after the high frequency low impact risk has occurred. The ordinary loss can be relatively small, but tail loss could have enormous influence on firms' abilities to operate. Many high profile losses in the financial industry have been traced to operational risk.

In 2008 a Finnish bank, Danske bank (formerly Sampo bank) faced difficulties with their new E-banking system. This online banking was aimed at customers and was not working properly. Changing the E-banking system contained varying levels of possible operational risks. Some of these risks occured and the improvement of the e-banking system did go as planned. This problem caused financial losses and a loss of customers. Some competitors claims that the loss of customers for Danske was as high as 40 000. Of course Danske bank denies this. This realized operational risk caused Danske bank customer and financial losses, but more importantly it caused irreparable reputational damage. (Taloussanomat, 2008)

A much more dramatic realized operational risk was the Enron scandal in 2001. The main feature of this scandal was its speed. Just a few months before bankruptcy, Enron Corporations was widely regarded as one of the most innovative, fastest-growing and best-managed firms in the United States. With hindsight it is clear that only the better side of Enron Corporation was visible to outsiders. The true condition of the firm was quite different. Issues in auditing, accounting, corporate governance and elsewhere led to the collapse of the Enron. The independent auditor made mistakes accidentally or possibly intentionally. In the accounting division the corporation's financial statements were formed in contravention of the rules of the financial statements of special purpose entities (SPEs). The company's board of directors failed in internal monitoring, which led to the possibility of internal frauds. These are all major operational risk and they are almost completely responsible for the bankruptcy of Enron Corporation.

2.2.3 Measuring Operational Risk

Firms in the financial sector are very good at measuring credit and market risk but measuring operational risk is much harder and a relatively new approach because operational risk is a rather new risk category and there is no "right" way to measure it.

Nevertheless, the financial industry wants to learn new quantitative approaches for operational risk. It is possible that a full quantitative approach may never be achieved but some techniques have already been identified in the theory of operational risk. Some stochastic methodology for quantitative analysis of certain types of operational loss data has been found. Only "certain types" of data are because not all operational risk data bend themselves easily to a full quantitative analysis. Operational risk data is very hard to put into a measurable form, for example it is almost impossible to know how much reputational damage is created by an individual realized operational risk. On the other hand legal risk fits much more comfortably in a quantitative analysis. The purpose of this chapter is to present operational risk measurement approaches. (Chavez-Demoulin et al. 2006)

Chavez-Demoulin et al. (2006) begin investigation of operational risk measurement with a well-known approach for risk measures and the development of advanced rating models for credit risk. Former practice to theory can also be expected to work in the area of operational risk. Basel 2 has work on the development of the Advanced Measurement Approach (AMA). AMA is one of the Basel 2 regulation standards for banks on operational risk. "Under the AMA approach, banks will have to integrate internal data with relevant external loss data, account for stress scenarios, and include in the modeling process factors which reflect the business environment and the internal control system." In 2014 only one bank in Nordic countries uses the AMA approach, SEB.

Chavez-Demoulin et al. (2006) based their research on the fact that banks collect data under AMA because operational loss events and loss random variables have to be well founded. For the calculations extreme value theory (EVT) is used because it is a useful tool for analyzing rare events and several operational risk classes possess properties which are naturally suitable for an EVT analysis. To aggregate data they use worst-VaR (Value-at-Risk) case. This means that data is aggregated with worst scenarios of the operational risk. They find that a clean standardized EVT approach is not available but generalization is possible and further study is needed.

Chavez-Demoulin et al. (2006) introduces operational risk measurement possibilities but finally just offer some new ways to approach operational risk measurements. Alexander Carol (2000) has a slightly different approach using Bayesian methods for measuring certain operational risk, such as transaction processing risks and human risks. The Bayesian methods come from Bayesian Belief Networks (BBNs). BBN dates back

to the late Reverend Thomas Bayes (1702-1761). In a letter he turned the view of basic assumptions in classical statistical models around. The question in classical statistical models is "what is the probability of my data, given that there is this true value fixed value in the data". Thomas Bayes' asked, "What is the probability of this parameter, given what I observed in the data". Every day there is more and more data in the world and that is the reason why Bayes' rule has garnered more attention. The main pillar of the Bayesian methods is the theorem of conditional probability of events X and Y. The basic equation is formed as follow:

Equation 1

$$prob(X\ and\ Y) = prob\ (X|\mathrm{Y})\ prob(Y) = prob(Y|X)prob(X)$$

Can be re-written according to Bayes' rule:

Equation 2

$$prob(X\,|\,Y) = (prob(Y\,|\,X)prob(X))/prob(Y)$$

A little example will make it more reasonable. Example is about measuring human risk, which is one of the most difficult operational risks to measure.

Lets suppose that you have a helpdesk where employers answer to the phone and help customers when needed. Because you are the manager of that team you have noticed with wide experience that 20 % of the time the team is providing unsatisfactory service. And when the team is working well and more efficiently, customer complaint data indicates that 70 % of clients would be satisfied. This leads to the fact that the probability of losing a client is 30 % when the team is working well. With your wide experience you have noticed also that when the team is working lazier the probability of losing a client rises as high as 60 %.

Now you have notice that the company has lose a client and you think were the team working well or bad. The probability of the helpdesk team providing unsatisfactory service is countable with the information above.

$$prob(Y) = prob\ (Y|X)\ prob(X) + prob(Y|\ not\ X)\ prob(\ not\ X)$$

Where, X = unsatisfactory service

Y = event "lose a client"

Your prior belief is that prob(X) =0,2

$$= 0{,}6 \times 0{,}20 + 0{,}3 \times 0{,}8 = 0{,}36$$

With Bayes' rule:

$$prob(X\,|\,Y) = (prob(Y\,|\,X)prob(X))/prob(Y)$$
$$= 0{,}60 \times 0{,}20 \div 0{,}36 = 0{,}33$$

With all this information the former belief that the team is not providing good service (20% of the time) is underestimation. Actually help desk team is providing inadequate service one third of the time.

Figure 3. Bayes rule. Source. Carol (2000)

This simple example of the Bayes' rule shows that with more study there could be more specific calculations for operational risk. For this reason the use of these kinds of causal networks to model operational risks has grown rather rapidly.

3. OPERATIONAL RISK MANAGEMENT

Managing risks lies at the heart of financial companies and for this reason more and more resources are allocated to risk management operations. Credit and market risk have received more attention in the past but now operational risk has been brought into consideration when building risk management strategy. Regulators such as Basel 2 for banking and Solvency 2 for insurance have been established to focus on operational risk. (Chavez-Demoulin, 2006) The largest banks have developed models to improve the internal management of operational processes and insurance companies have created products for operational risk. Operational risk management will soon join credit and market risk as one of the main categories of risk management, if it has not already done so. (Carol, 2000)

3.1 Identifying Operational Risk

Which should companies focus on: low frequency high impact risk, or high frequency low impact risk? Some claim that, focus on low frequency high impact risk is much more important because the realization of high impact operational risk could be fatal if the company has not prepared for it. Others claim that high frequency low impact risk, when aggregated, could cause major damage to the company. This, however, is just one way to approach operational risks. There are numerous ways to identify operational risk and the initial perspective shows the direction. In this chapter I will introduce a couple of ways in which companies in the financial sector identify their operational risks. (Alexander Carol, 2000)

In the past, we have witnessed realized operational risk such as frauds, legal deals going wrong, technological failures and smaller errors such as system breaks or failures caused by untrained staff. For a company it is important to recognize these kinds of operational risk and be prepared if they are realized. Perhaps the most famous case of fraud was committed by Bernard Madoff whose ponzi scheme was one of the biggest frauds in the history of finance (over 50 billion US dollars). The reason I have brought this up is that it affected many financial companies but, with proper operational risk management, this fraud could have been avoided or at least noticed earlier. Gregoriou and Lhabitant (2009) investigated the Madoff scandal and found there were salient operational features common to best-of-breed hedge funds that were clearly missing

from Madoff's operations. This means that with proper quantitative analysis someone should have identified the incompleteness of Madoff's operations. The surveillance failed over and over again and Madoff continued making money with the ponzi scheme. The main issue was that there was no third party oversight and no third party to independently confirm the legal ownership of the fund's securities. This made performance manipulation possible. Furthermore, Madoff used a very small auditor, this should obviously have raised doubts. By contrast, Madoff also used large, reputable audit firms, which probably reassured investors.

The list of these kinds of "red flags" is long, but still Madoff proceeded for almost two decades. If internal and external controls had been effective, this ponzi scheme might not have occurred, at least not to such an extent. (Gregoriou and Lhabitant 2009) Avoiding internal and external fraud is one of the key functions of operational risk management. Madoff created his empire from nothing and maybe internal controls failed because Madoff himself was above all investigations.

From the perspective of an operational risk manager, identifying rogue trading from the beginning is more important. A rogue trader is a trader who usually trades with high risk, high reward investment, but does not have permission to do it. A rogue trader is a gambler who plays with money from the institution that employs him. In the biggest cases of rogue trading the employer has usually been a big bank.

The world's most famous rogue trader is Nick Leeson who worked for Britain's Barings Bank at the Singapore office. Leeson invested very large amounts of money in Nikkei futures and options, almost 3 billion dollars. These investments were unauthorized and Leeson managed the whole investment himself. When the Nikkei experienced a downturn Barings bank lost over 1 billion dollars and fell into bankruptcy. One man caused the bankruptcy of a more than 200 year old bank which was, at that time, the biggest bank in the world. This could have been avoided with better internal control. As we now know realized operational risks can cause major damage to a company and even bankruptcy. Another rogue trader was caught in 2011, his name is Kweku Adoboli. Adoboli made off-the-books trades that at one point were worth more than 7 billion pounds. Ultimately Adoboli caused over 1.5 billion pounds worth of losses to UBS (Union Bank of Switzerland).

UBS has also been a participant in a different kind of realized operational risk. They were involved in the manipulation of Libor (London Interbank Offered Rate) rates.

UBS, along with five other banks (Citigroup, Deutsche Bank, HSBC, JPMorgan and RBS) have admitted their involvement in the manipulation of LIBOR rates. (Rosa M. Abrantes-Metz, Michael Kraten, Albert D. Metz & Gim S. Seow, 2012)

How can financial institutions find these operational risks before it is too late? Knowing what will happen in the future is impossible, but preparing for the future is achievable and strongly recommended. One way to forecast the future is to look at historical evidence. Unfortunately there is not as much historical operational risk data as credit and market risk data. Although companies have recently started to collect data such as loss events data, it is still far from the historical data that is possessed concerning credit market risks.

3.2 Managing Operational Risk

Douglas G. Hoffman sums up operational risk as: "operational risks are those of our interconnected world becoming disrupted on a large scale, or locally in our workplaces or neighborhoods through acts of man, or of nature." They can occur through careless omission and co-workers' mistakes, or frauds causing massive damage to our companies. According to Hoffman, operational risk usually lies in wait, quietly hidden most of the time. Large operational risk occurs far less frequently than small operational risk and this makes large operational risks more dangerous. This situation causes management to ignore and underestimate large operational risk, creating one of the challenges of managing operational risk. Operational risk management should be a balance between reasonable control and overbearing control of large-scale operational risk.

Dr. Jacques Pezier divides operational risks into three different broad sections: Nominal, Ordinary and Exceptional. The nominal operational risk is the risk of repeated losses, losses that may occur once a week or more frequently. A practical example could be human error in a transaction processing. According to Pezier, these kinds of losses hardly deserve to be called risks. He thinks that they should rather be compared to the cost of controls. Although the nominal risks are quite small, the losses are very expensive. If the company improves procedures and creates a better quality culture, it often creates savings immediately and also gains beneficial long term effects on reputation and client relationships. Therefore nominal operational risk should be taken into consideration when creating operational risk strategy.

Ordinary operational risks losses occur less frequently but create larger costs, yet are not life threatening for financial institutions. They are often the result of several independent strategic choices and therefore should be analyzed within the wider context of those choices.

The third operational risk that Pezier created is exceptional operational risks. These risks rarely occur but may be life threatening to financial institutions. These risks deserve special attention.

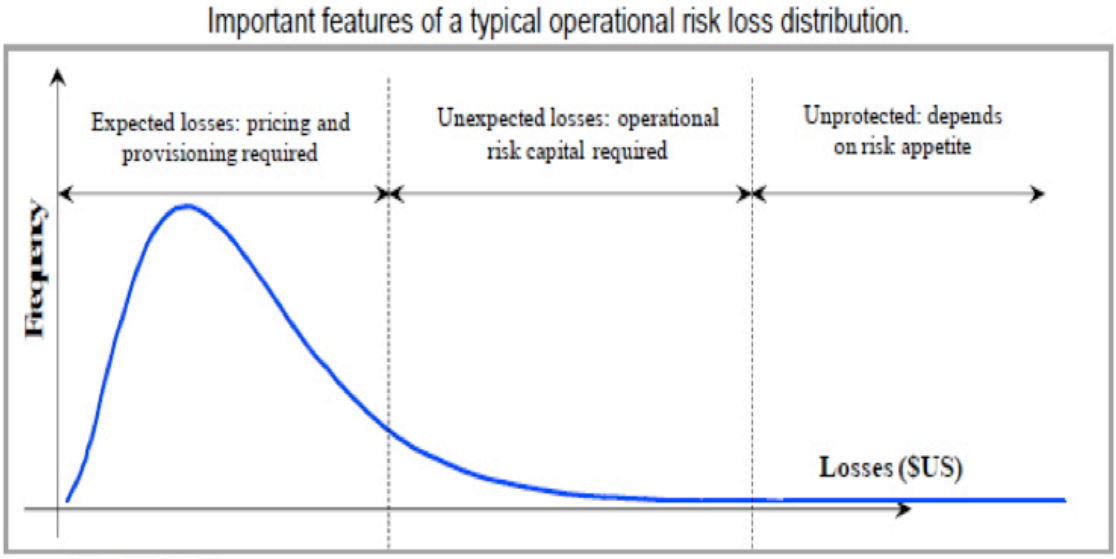

Figure 4. Operational risk loss distribution. Source: Cruz (2002)

The diagram above shows the relationship between frequency and losses. As we can see, high frequency low impact risks occur more often and those risks are not yet dangerous to a company. But still there is the opportunity to create savings when managing risks correctly. The higher the loss, the lower the frequency is. This is normal when dealing with risk generally. When the line moves towards the right, frequency drops and these risks are life threatening to a company.

The probability of exceptional risks occurring is very low but they can be life-threatening to financial institutions. These risks deserve special attention. Large banks and financial institutions carry out scenario analyses to identify exceptional risks. Actually the AMA approach is also a tool for scenario analysis. (Chavez-Demoulin et al. 2006) Low frequency, high impact operational risk events are of particular interest to operational risk managers or at least should be. (Jobst, 2007)

Although high impact losses are crucial to companies, it is very important to manage high frequency low impact risks also. This is because of the tail events. Tail events are typically formed after the occurrence of minor operational risk. The minor risk provides the opportunity for other operational risks and when this continues the final impact could be at a major loss level. Basel 2 requires banks to target their attention on unexpected losses (low frequency high impact) and tail events. Banks have to capture tail events before they become excessive. (Esterhuysen et. all. 2010) Nevertheless insurance companies have still not received the same kind of regulations from Solvency 2 and need to wait for the release of regulations in 2015. Although there are no comprehensive operational risk regulations for insurance companies, some use Basel 2 instructions as an indicative guide. Bank regulators (Basel Committee) are and will be trailblazers in operational risk management.

4. QUALITATIVE METHODS

Because my main study focuses on the interviews I have carried out, it is important to become familiar with qualitative methods. Data gathering from interviews is still the most common method in qualitative research such as this. In qualitative interviews the interviewee is seen as a participant of the study, unlike quantitative interviews where the interviewee is seen as a research subject and the relationship between interviewer and interviewee should be minimized to avoid the impact of inter-personal processes. A qualitative researcher believes that the relationship between interviewer and interviewee is important and provides every single interview with unique answers. The interviewee should respond to questions actively rather than passively. The relationship between interviewee and interviewer is the key feature of the qualitative research. (Cassel & Symon, 2004)

4.1 Interviews

Interviews can be done face-to-face, by telephone or even via the Internet. Of course the best result usually comes from face-to-face interviews. When interviewing face-to-face the relationship between interviewer and interviewee is much more authentic and usually gives better quality answers. Selecting interviewees for qualitative research is usually nonrandom and a small sample, as in this study.

4.2 Qualitative Research

In qualitative research the researcher has a huge responsibility for how to analyze the results from interviews. It is inevitable that the researcher's own knowledge and perspective comes into the picture when analyzing results. This is one of the reasons why, throughout history, scholars have argued whether research is and whether it creates a credibility problem when an individual analyst interprets results. However Madill et al. (2000) conclude that it does not matter as long as the researcher makes his/her relationship with the material clear. So the challenge for the qualitative researcher is to show that personal interest will not bias the study. (Marshall & Rossman, 1998) The researcher could have, for example, a political agenda which might reduce the credibility of the study. In this study there is no political agenda or any other agenda which could influence the integrity of the study.

Unlike quantitative research, qualitative research is not based on calculations or pure data like stock values of a particular firm within a particular timeframe. Qualitative research does not give measurement and analysis of the causal relationship between variables but the processes and socially constructed nature of reality. (Denzin & Lincoln, 2011) In this chapter the main focus is on what is qualitative research. The war between qualitative and quantitative research has been set aside.

With qualitative study the researcher is trying to determine the cause of events and after that focus on predicting similar events in the future. Qualitative research is often chosen because there is a lack of theory or an existing theory fails to completely explain a phenomenon. The researcher gathers data to build hypotheses or theories and rarely tests former hypotheses. Understanding observations and interviews is very important when trying to build hypotheses. The qualitative researcher uses words and pictures rather than numbers when addressing the phenomenon. The data collected is treated with equal weight. This means that all pieces of the data have equal value during analysis. In this case the major part of the data comes from interviews. (Denzin & Lincoln, 2011)

This qualitative research aims at identifying key operational risks in a Finnish insurance company with help from the interviews. Interviews also assist when investigating the most common tools used in operational risk management in the insurance business in Finland. Finally, the interviews give perspective on the question of how Finnish insurance companies prioritize resources between different operational risks. The data collected from the interviews should be enough to create a helpful guide for operational risk management.

5. OVERVIEW OF THE INSURANCE BUSINESS

The insurance business has been around as long as people have had property or assets to protect and can be traced back almost 5000 years. 5000 years ago, Chinese traders protected their cargo with primitive diversification when they had to cross a dangerous river. A thousand years later, Babylonians created a more modern profit insurance business. The lender offered insurance against robbery to a borrower in exchange for higher interest rates. The first insurance companies were formed after the great fire of London in 1666. The past of the insurance business has created the foundations of today's insurance companies and their operating practices. This chapter describes the basics of the insurance business today in general, in Finland and in Company X. (RandMark40)

5.1 Insurance Business

A human has always wanted to cover its back. This is one reason why the insurance business is a tremendously large financial sector. Everybody wants to be prepared for when something goes wrong. Harris Schlesinger from the University of Alabama wrote an article on The Theory of Insurance Demand (2013). Insurance demand is said to be "the purest example of economic behavior under uncertainty". Uncertainty is very important feature of the economic world today. The world is living in a constant cloud of uncertainty but if this uncertainty grows too quickly and too much, it may trigger an economic downturn. Insurance companies benefit from balanced uncertainty, but like other financial sectors, the insurance sector too suffers in an economic downturn. For the insurance sector a downturn means an increase in payments of compensation and a decrease in new business.

The theory of insurance demand does not deal with the trading risk, but with a personal risk. Personal risk originates from the consumer's individual life. The consumer could try to find other similar consumers, who could share the same type of personal risk. They could try to pool risks with a large group of consumers, but it would be difficult. Insurance companies organize these pools for consumers so it is only needed to join the pool rather than create one. (Harris Schlesinger 2013)

Insurance can be considered as a financial asset. Unlike most financial assets, insurance is a contract contingent on the individual's own personal financial circumstances and is therefore non tradable. Although insurance can be considered as a financial asset this personal nature of the contract separates it from other financial assets. The basic idea of insurance is very simple, although the contract could be rather complicated. For example, the consumer pays a fixed premium and, in return, the insurer will pay the insured a sum of money dependent on the value of a loss that the consumer has suffered. (Harris Schlesinger 2013)

Moving on from the insurance business, it is time to focus on the business sector itself. The world's three largest life insurance companies 2015 in terms of total assets are AXA from France (US $1.022 bn), Allianz from Germany (US $0.98 bn) and MetLife United States (US $0.902. The number one life insurance company from the USA is MetLife (ranked fourth in the world with US $0.837 bn). Company X total assets are worth US $0.108 bn. MetLife is almost eight times bigger that Company X. (The Statistic Portal, 2014)

"The insurance business is nowadays a combination of information and technology, both of which are critical cornerstones for successful operation." (Järvinen Raija, Lehtinen Uolevi and Vuorinen Ismo, 1998.)

5.2 Insurance Business in Finland

The basics of the insurance business in Finland are the same as everywhere else although in the Nordic countries social security has been organized according to the Nordic welfare state model. This model guarantees basic living security, rights to public services and income security. The minimum security is financed by tax assets and aimed at those who cannot obtain enough income otherwise. From a global point of view, the minimum security level is slightly better in Finland than the Western European average. The Finnish government takes care of the minimum security and statutory health insurance. Car insurance and work injury insurance have been organized by private insurance companies. The majority of the population working in the private sector has statutory pension insurance from private pension insurance companies such as Ilmarinen Mutual Pension Insurance Company. (Sosiaali- ja Terveysministeriö, 2015)

The primary part of social security is the occupational pension. This covers invalidity, retirement and a spouse or parent's death. National pensions and guarantee pensions are financed completely by taxes, these guarantee pensions secure a minimum income if the occupational pension is too small or not accumulated at all. The guarantee pension is paid to people whose total pension is less than the full guaranteed pension. The full guaranteed pension in 2015 is 746,57 euros per month. All people living permanently in Finland are insured against sickness. Employers, employees and the state finance health insurance together. In Finland, all employees are also insured against unemployment. The state, employers and employees fund unemployment insurance. (Sosiaali- ja Terveysministeriö, 2015)

There are approximately three different types of private insurance companies in Finland, mutual pension insurance companies, health insurance companies and damage insurance companies. In 2013 the balance sheet value of all Finnish insurance companies was 114.5 billion euros, of which 70% was mutual pension insurance companies' share. The total gross premium was 22 billion euros, where mutual pension insurance companies' share was 12 billion euros. (Tilastokeskus, 2013)

5.3 Company X

Company X is a financial security company from the USA that provides insurance, wealth management, investment and financial solutions. This holding company has over 15 million customers in more than 25 different countries and over 600 institutional partners. It all started in 1871 as The Life Insurance Company of Virginia. In 1986 it was sold to Combined Insurance, later known as Aon. Almost a decade later in 1996, Life of Virginia was sold to GE Capital and 8 years after that GE Capital formed Company X from the various insurance businesses of General Electric. This was the USA's largest IPO of 2004. Company X is a Fortune 500 company and in 2013 it had a turnover of 9.4 billion US dollars, with an operating profit of 560 million dollars. In the whole corporation there are almost 6000 employees. Standard & Poor's has given Lifestyle Protection credit rating "A".

Lifestyle Protection markets a range of life insurance, long-term care insurance and fixed annuities. The company offers universal life insurance products which provide permanent protection for the life of the insured. Protection from illness, accident,

involuntary unemployment, disability and death are the primary insurance products of Lifestyle Protection.

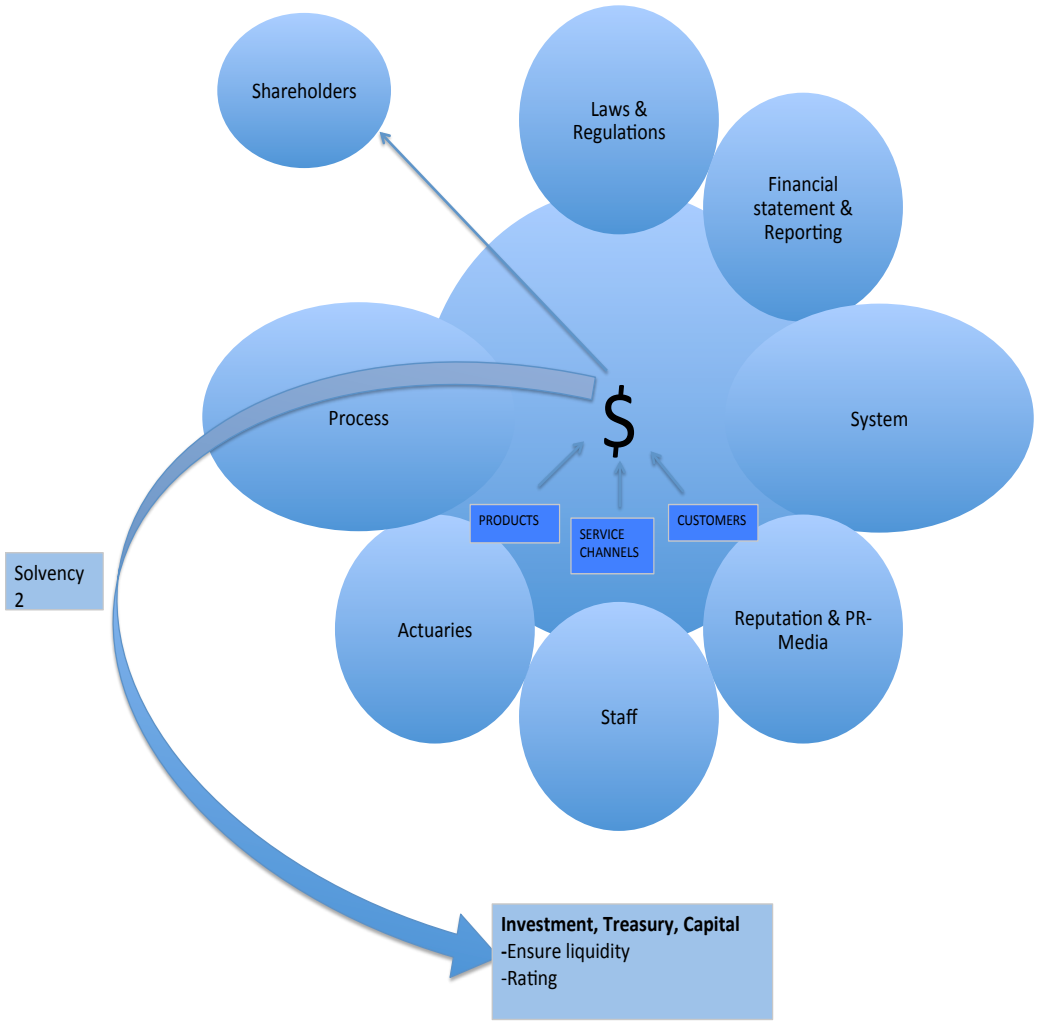

Figure 5. Organization structure of Company X

Figure 5 above shows the structure of the Company X branch. In the middle there is a dollar sign, which refers to the fact that processes, staff, shareholders etc. are driven by money. To make a profit, Company X needs good products, well-managed customer channels and loyal customers. To make these three particles work efficiently we need skilled employees, functional processes and systems as well as professional actuaries. In addition, laws and regulations must be obeyed and financial reporting must be flawless. An essential part of a life insurance company is reputation. Without a reliable reputation an insurance company has too large a burden to carry. The reputation is made with proper marketing but it is especially created by an attitude of doing things well and treating customer fairly. There are two lines leaving from the dollar mark, shareholders

and “Investment, Treasury, Capital”. Shareholders demand return on their investment and in order to grow the company has to make investments. In the middle of the longer line stands Solvency 2 which has made some regulations for the insurance business. Due to capital requirement regulations for example, money stays in the reserves and cannot be invested. In the future, regulations might have more impact on the insurance business as Solvency 2 will be published in 2015.

6. DETECTING OPERATIONAL RISKS CASE: FINLAND / COMPANY X

For the interviews I used an open-ended questionnaire. This proved to be the right choice when dealing with operational risks because operational risk management is still on a relatively low level and the operational risks affecting companies' processes are identified in everyday tasks. Almost every employee somehow affects operational risk decisions. Of course large impact decisions are made at a senior management level.

For example, typos are usually identified through controls but if there are no controls for a particular typo, an employee can refer it to a direct superior who can take the matter further and a control may be introduced in the future. This is a textbook example of low level action for operational risk management. Operational risk management is so broad that everybody participates in it in some way.

In this digitalizing world, by far the most important point raised was technological development with system problems and system implementations. The insurance sector is particularly dependent on information systems. Insurance companies operate with information technology and if this does not work properly a company can say goodbye to its customers at an alarming rate. However, information technology was not the only operational risk raised in the interviews. In this chapter I will present and analyze the results from interviews.

6.1 Data

The data collected is from interviewed employers and managers from Finnish insurance companies and banks. Open-ended questionnaires were structured with 12 open questions. Questions were similar in both questionnaires, as shown below. The idea was to investigate operational risks in three time dimensions: past operational risks, present operational risks and future operational risks. A further aim was to examine what tools are used to manage these risks. The internal questionnaire was for interviewees from every section of Company X and so the responses are more diverse, although internal interviewees were not working directly with operational risks.

The credibility of the external questionnaire is based on the fact that every interviewee was a professional in operational risk management and therefore an appropriate person to analyze operational risks.

I have interviewed 9 people from Company X. One of these people is working with operational risks and eight have an impact on operational risk management. In addition, I have interviewed 5 people outside Company X. All of these people are professional operational risk managers who deal with operational risks daily. They are from are other insurance companies in Finland. The interviews were carried out in Finnish and then translated into English.

"There is no point worrying about things that cannot be controlled nor any commercial value in gathering information unless it may affect some decisions." (Pezier, 2002) No commercial value in gathering information unless it may affect some decision. Answers from interviews support this statement. Companies gather information about operational risks with "loss events" recordings or realized operational risks recordings. Credit and market risk data has been collected in abundance. Credit and market risk have enjoyed years of a standardized, globally applied, methodological approach. Internal operational risk data, however, is far from abundant even for most banks.

Chapter 7.2 will present all the answers from the questionnaire. There will be differences and similarities between practice and theory and between different types of insurance companies. The answers will be allocated to categories or groups to help understand the relationship between different operational risks. The true value of this section is to create ideas and issues for further research.

6.2 Internal Questionnaire

When working with interviews it is important to realize that recent events will certainly have an impact on the interviewees' responses but as we are dealing with operational risk it is more than welcome. As I have previously mentioned, everybody can be involved in operational risk management, operational risks occur in everyday tasks, and change with time. The more recent the realized operational risks, the closer we get to the optimal situation. The questions are not always presented in the same order as in the questionnaire because some questions are interrelated so are presented consecutively in order to facilitate understanding. All the internal interviews were held in the summer of

2014 when there were minor problems with the system in Company X. As a result, many similar points emerged. In question six, interviewees were asked about operational risks in their former workplace and how the tools used differed from the tools used at Company X. Unfortunately the answers remained too fragmented and deficient to bring any added value to this study therefore question number six will be excluded from the analysis of the questionnaire.

Each of the nine interviewees mentioned the functionality of the system. There was a system stabilization project going on at that time, which probably meant that this topic was discussed more. Functionality of the system is, however, also one of the topics raised recently by researchers and external interviewees. Our current era is very technology-dependent and therefore concerns about the functionality of systems are pertinent. One of the questions that asked of the interviewees was: How great a risk/threat is the development of technology and your company's constantly growing dependence on it? The answers were quite interesting, as you can see from table 3. The answers are organized very simply into two categories, yes and no, with justifications. The numbers after the answer are number of responses.

Four people said that it is a risk because of underdevelopment which creates risks for the company, three people think that if the company does not develop someone else will. The total of seven answers indicates that if the company does not react to technological development, it will face hard times ahead. This is one of the major risks in technological development. The generation born two decades ago, commonly known as a wired generation, demands services via the Internet. Windsor Holden put it nicely, "Young people have seen all these different facilities, adapted them and changed the means of communication." The whole communication system is changing and companies have to be able to provide services in quickly updating channels. This means that if a company cannot keep up with development it has no future, or at least the future does not look very bright. But is this an operational risk, a business risk or even a strategic risk? It could be a strategic risk if a company's management saw it as a normal option not as a mandatory decision. Of course there are strategic risks when service providers are selected, but actually being able to meet the demand of technological development is no strategic decision. Is it then a business risk? Business risk is very close to strategic risk but there remain some slight differences.

This table shows the answers to the question: How great a risk/threat is the development of technology and your company's growing dependence on it? The answers are divided into yes with justifications and no with justifications. "Replies" show the number of the answers.

Table 3. How great risk/threat is the development of the technology and its constantly growing dependence to your company?

Arguments for yes	Replies	Arguments for no	Replies
Underdevelopment creates risks	4	Decreases operational risk, if done right	4
Hacking	3	Working would be more effective and easier-->reducing operational risk and open up new opportunities	3
If we do not develop someone else will	3	Less manual work--> less human risk	2
Functionality of the information system before the development doubtful	2	The more automated the better --> less mistakes--> less risk	2
Multiplied dependence--> growth in operational risks	1	It can create new approaches to processes	1
If there are unskilled people to make changes. They have to be able to see the big picture of the change (which changes have a bigger influence.	1	Easier risk management approaches	1
Very small mistake can cause very big problems	1		
Pressure that more comprehensive technology will fail	1		
	16		13

Which company is selected to help with information technology development is a business decision and creates business risks. Since the decision is mandatory, as mentioned before every company has to develop old information systems, and based on responses from interviewees and previous literature, I would say that it is a business risk which creates operational risks. It will also create external operational risks. If the selected supplier proves to be ineligible, it could cause substantial consequences. For example, when an insurance company has bought information technology services from a company that suddenly suffers crucial losses and therefore can no longer offer services. For this reason an insurance company has to think twice before outsourcing.

Yet again the outsourcing decision is a business decision, which creates possible operational risks.

On the contrary, four answers responded that technological development does not increase operational risks, if done correctly. This answer is supported with other no category answers; if the technological development is done correctly there will be less manual work, which means less human risk (2 answers). Also better information technology makes working more efficient and easier, which reduces operational risk and opens up more time for employees to focus on something else (3). Battling with a poor system reduces effectiveness significantly. Reducing operational risks with better information systems makes the operational risk management job more systematic (2) because operational risks are easier to control if there is no room for human error. Overall the more automated the system, the less room there is for human error and the less generation of operational risks (2).

More than half of the responses expressed concerns about technological development. There were multiple reasons for concern. Many said in the interviews that technical development removes certain kinds of operational risks, but new operational risks take their place. Hacking came up three times, which is quite a small number considering that there have been several large-scale information leaks recently, such as Julian Assange or Raphael Grey. The insurance business, however, has remained relatively untouched by hackers, which was reflected in the answers. The one thing that hackers could steal is people's personal information, which is still difficult to make use of. In addition, criminals' interest is money and insurance companies do not deal with money in the same way as banks do. As it is extremely difficult to steal money straight from accounts, insurance companies have been left untouched. Prevention of operational risk caused by hacking is done with firewalls. The desired strength and coverage of the firewall depends on what resources management are willing to allocate to it. Losses caused by hackers are more or less in the form of reputational damage, nevertheless losses to insurance companies from hacking could need further research.

The pressure that more comprehensive information technology will fail is mentioned in the answers only once. The same kind of argument is that very small mistakes can cause very big problems and comprehensive information technology will cause multiplied dependence. This means that there is a fear that information-technology's role in the company's everyday tasks is growing beyond people's understanding. This is a reasonable concern but, as previously mentioned, technological development is

mandatory and therefore it is very important to do it right and not only cover a system's deficiencies without looking at the big picture. This topic was raised in the context of almost every question so the importance of information technology will unfold during this section.

In the questionnaire there are three simple questions where interviewees name operational risks. In addition, there is a question where interviewees name operational risks from the past, present and future. The answers of these questions have been put in a four-field matrix where the fields are system, people, processes and regulations, and external risks. Simply, risk caused by a system goes into the system field, risk caused by people goes to the people field, risk caused by failed or inadequate processes goes to the processes field and risk caused by regulations or external events goes to the last field.

6.2.1 Single operational risks in four-fielded matrixes

After checking whether the interviewee is familiar with the term operational risk, the second question was: would you mention a few realized operational risks that have occurred in Finland or worldwide? Again, information technology was by far the most popular answer. Everyone mentioned that the stabilization of the system is an operational risk that Company X is facing. The four-field matrix below is formed with the answers of question 2 so that the size of the figure depends on how many people have brought it up and the location of the figure depends on which category it is suitable for. For example, stabilization of the system is the biggest figure and it belongs to systems. However if some of the topics fit in both system and people or processes and system etc. it goes between those fields depending which has the stronger influence.

Stabilization of the system was the one of the most mentioned subjects in this question and was brought up very often in the other questions too. This indicates the concerns about old and new systems and their functionality. System is also one of the four areas in the matrix and it is no coincidence that it is in people's minds nowadays. Of course system stabilization is a relatively large part of systems and may be mentioned so often for this reason. Without going deeper into the letter problem, it can be said to be the result of failed internal testing and the complexity of the system. Failed internal testing moves the ellipse number two towards process and people. This means that the reasons behind this operational risk are also in failed processes and human error, not only the system.

The list above is formed from the answers of the interviewees in question 2. Answers have been put in to the four-field matrix so that the bigger ellipse the more references it has received. Also the location of an ellipse depends on which category it belongs to most.

1. Stabilization of the system
2. Letter Problems
3. Rogue traders
4. Subprime loan crisis
5. Failed data protection
6. Hacking (passwords)
7. Healthcare Norway
8. Bhopal
9. Mis-sold products (England)
10. Talvivaara
11. Enron scandal
12. Malaysian airlines
13. Russian constraints
14. Sonera deals in Germany
15. Nokia

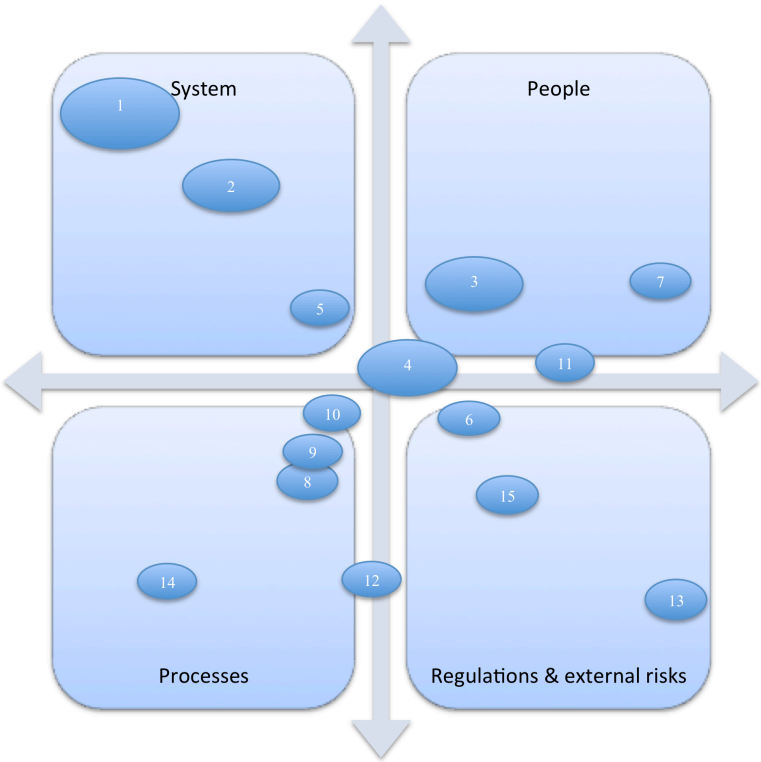

Figure 6. Would you mention a few realized operational risks that have occurred in Finland or worldwide?

Like letter problems, there are many other similar individual realized operational risks, which are in the matrix. These individual operational risks are mentioned only one time and one reasonable explanation for this is that there are countless numbers of similar

realized operational risks in the world and it would have been just a coincidence if two or more interviewees had mentioned the same unique operational risk.
The third question was: What kind of daily operational risks does your company face? Again stabilization of the system was the most cited operational risk. This was not a

surprise because employees work with the system daily and if the system is not working properly their work becomes a lot more difficult. Unlike question two, question three raised operational risks caused by people. Six interviewees brought up mistakes that people make and five interviewees brought up human risk. In this case, human risk is the risk that is caused as a result of limited resources. For example, if an expert is on sick leave and problems occur or the only person who might be able to help is not available. Therefore it is important that no single work is without a back-up person. If there is no back-up person the damage can "leak" somewhere else or multiply and create more operational risks.

Let's create a hypothetical situation where the IT expert is on sick leave and there is no replacement present. Now system errors have occurred and the employee (let's call him John) in the claims service is not able to log in to his computer. Because John cannot log in to his computer, numerous applications for compensation from customers will not be handled and payments to customers cannot be made. Customers do not receive their payments, which they are expecting, causing resentment and reputational damage. Why would you buy insurance if the insurance company cannot pay compensation? Late payments and slow processing are not a good advertisement for an insurance company. Of course this kind of unpleasant situation needs realized human risk and errors in the system but this is what risk management is all about. Should we hire two IT guys to make it more unlikely that IT support is not available or is it too expensive compared to the risk that is created by having only one IT person.

Nevertheless risk caused by human error was given a lot of attention in this question. When going a little deeper, interviewees related single examples of the risks caused by mistakes. Classic operational risks mentioned were mistakes in phone services, accounting errors, accidental false promises and the misinterpretation of the terms of compensation. In addition, bad communication and mis-priced products were mentioned. The largest ellipses are in the fields of system and people but regulation external risks, as well as processes, have not been ignored. The main point in the four-field matrix below, when comparing these answers to other matrices and external answers, is the location of the ellipses.

1. Letter problems
2. Staying with the digitalization
3. Mailing problems
4. Reminder invoices
5. Failed data protection
6. Interruption of the functions
7. Payment transactions
8. Stabilization of the system
9. Supplier risk/partner risk
10. Misinterpretation of the terms of compensation
11. Accidently false promises
12. Mis-priced products
13. Accounting
14. Mistakes in phone services
15. Partners mis-selling products
16. Poor instructions
17. Mistakes of the people
18. Communication
19. Following the budget
20. Problems in the processes
21. Controls
22. SLA
23. Blackouts/fire/burglary
24. Terms too open to interpretation
25. Global economic situation
26. Reputational risk
27. Limited resources
28. Human risk

The list above is formed from the answers of the interviewees to question 3. Answers have been put in the four-field matrix so that the bigger the ellipse the more references it has received. Also the location of an ellipse depends on which category it belongs to most.

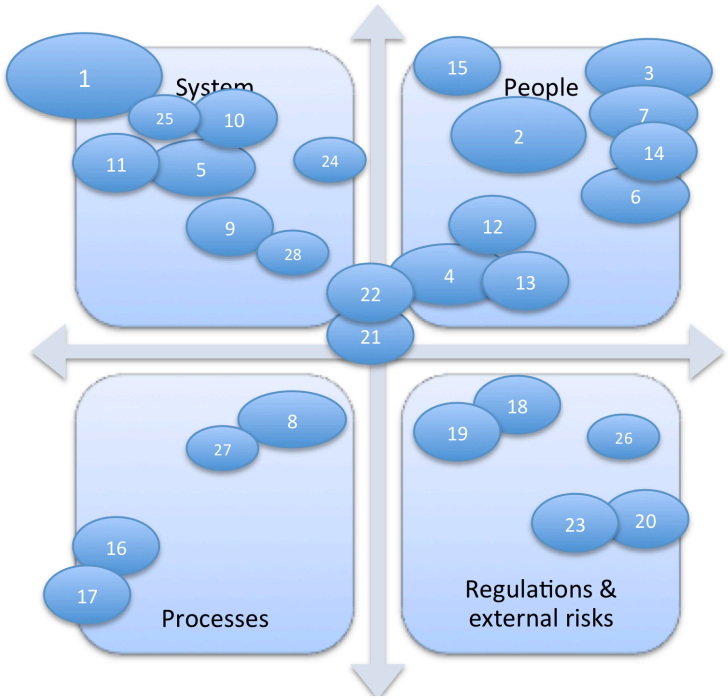

Figure 7. What kind of daily operational risks does your company face?

When comparing these two matrices above, the number of different operational risk events is striking. Interviewees mentioned many more single events when it comes to

their own company. The ellipses in the second matrix clearly focus on the system and people. The sizes of the ellipses are larger in system and people too. This indicates that operational risks caused by systems or people are more common in everyday tasks than risks caused by regulations and external risks, or processes but this is rather usual in the theory of operational risk. Operational risks caused by people are usually minor risks and they occur more often. Answers concerning the system can be explained by today's system-dependent working habits. People are working with the system every day and if the system is not working properly productivity suffers. A poorly functioning system causes operational risks every day.

However, the four biggest single events were stabilization of the system (9), human error (6), human risks (5) and communication (4). Human error and human risks can simply be put in the people section, but communication is a bit more complex. Communication usually means interaction between coworkers or between employees in general. Nevertheless communication includes processes as well. If the processes are not solid, communication can be weak. Let's look at the simple process where an employee discusses with a customer via e-mail and does not include any other notes or documents. This particular employee then resigns and his or her e-mail is removed. This kind of case could cause a situation where there is no evidence of what has been agreed. But if an employee writes down this agreed matter in a shared folder where everybody can check later, the above-mentioned situation does not arise. Without proper processes communication can be poor and so communication is placed towards processes, although it is still people who communicate with each other.

Let's go back to the case where information is lost because of failed processes. This kind of situation may cause the loss a customer and, even worse, it can create broad reputational damage if the customer, for example, shares his/her experiences on social media or the media in general. Every event that directly or indirectly affects customers creates or, at least may create, reputational damage. For this reason, reputational damage needs to be taken into consideration almost every time when an operational risk occurs and of course before the risk is realized.

The list below is formed from the answers of the interviewees to question 11. Answers have been put in to the four-field matrix so that the bigger the ellipse the more references it has received. Also the location of an ellipse depends on which category it belongs to most.

1. Digital innovations
2. Systems in general
3. Communication
4. Lack of risk assessment
5. Better operating systems for customers
6. Competitors ahead in digitalization
7. Mis-sold products
8. Hacking
9. Human risks
10. Information security
11. Increasing longevity
12. Reputational damage caused by human mistakes
13. Service providers/channels of distribution
14. Limited sale channels
15. Skilled labor hard to get
16. Systematization
17. EU amendment
18. Company for sale
19. Unable to follow the change
20. Investment operation failure
21. Agreements must be long-term
22. Industry competitors
23. Regulations

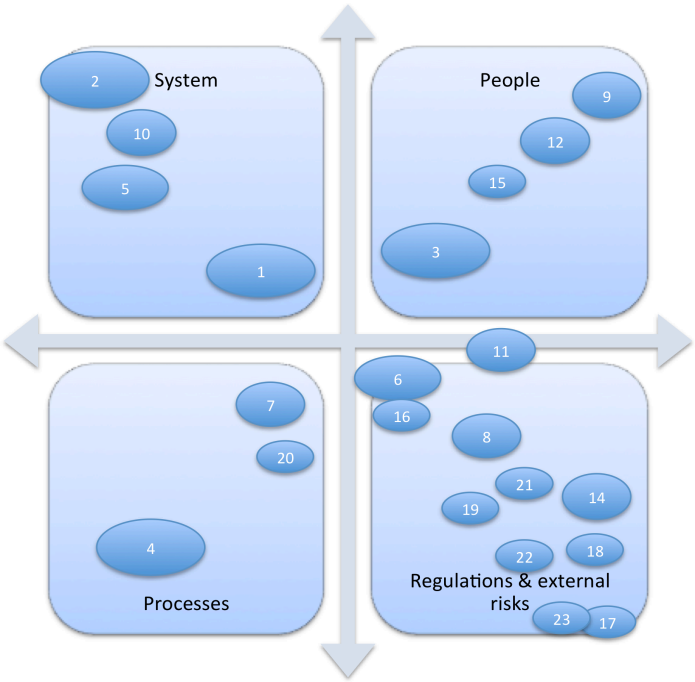

Figure 8. What is in your opinion the single largest realized operational risk? And how do you think it could have been prevented?

The third four-field matrix is formed on the basis of the 11th question on possible operational risks that could happen in the future. Now the answers started to move

towards the field of regulation and external risks. This could mean that regulation and external risks concern people more than, for example, risks caused by humans. There are two big ellipses in the system field system in general (2) and digital innovations (1). Interviewees believe that operational risks caused by systems will be important in the future as well as today. Digital innovations move towards external risks because external parties are expected to set requirements for digital developments, then companies try to keep up with the development. This causes very big operational risks, for example, when the company decides to renew their information technology. The next figure displays what kind of different operational risks might possibly arise when renewing information technology. The decision to renew information technology is no operational risk itself but it can, and often will, create different kinds of operational risks. It is very common that one operational risk creates another when realized and it is essential to understand what those risks are. It is highly unlikely that all of the risks or events in figure seven would become real, but one should still be aware of the risks.

As we can see from the figure below, renewing information technology can create a large number of operational risks. It is risk management's duty to analyze which operational risks in the figure the company should pay attention to, manage, entirely avoid or leave alone because of the resources spend with respect to the losses that realized operational risk could cause.

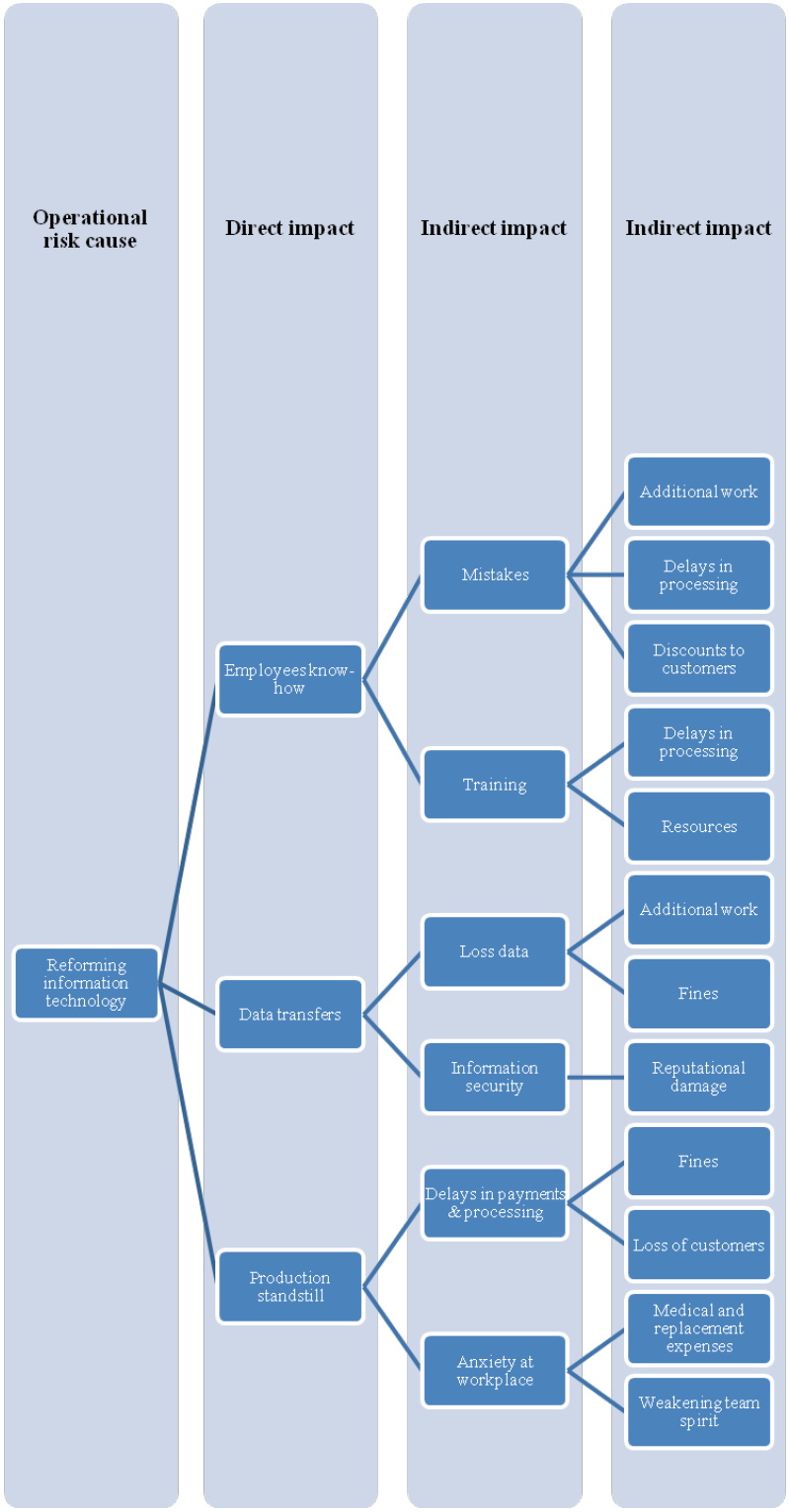

Figure 9. Reforming information technology

6.2.2 Identification, calculation and prioritizing operational risks

In the table four there are eight different events that can create operational risks. Events are picked up from the matrixes into rather different example to introduce the risks. The idea of the table is to go deeper in the risk. What might be the consequences and the expenses of the risks? Some of the risks are minor and some of them are quite broad. As we can see almost always one of the expenses is reputational damage. The "fact" that all kind of publicity is in favor does not apply for insurance companies. However it is very important to a company to discuss somewhat like this to make sure that all possible consequences are known and understood. Because having full knowledge of the risks that the firm is taking is a fundamental pillar of the operational risk management. Every company should clarify what are consequences of different operational risks. It is obvious that different business sectors have different operational risks and different consequences after an operational risk has occurred. Nevertheless in life insurance business there are quite similar operational risks despite which Life Insurance Company is selected.

The last sector in the table 4 is an example how companies could analyze their risks. First number is probability of the risk and second number is expense of the risk. Numbers have been categorized 1-3 so that number 1 is low probability, number 2 is medium probability and number 3 is high probability. Second number is expense and the system is same in here, number 1 is low expense, number 2 is medium expense and number 3 is high expense. When operational risk managers have discussed and decided on which risks get which numbers they can focus on those risks that have obtained larger numbers in both categories. For example 3+3 is high volatility high impact risk so the company should invest more time and resources to manage it. Actually company should never drift into situation where there is high impact high volatility risk. It is also highly unusual that firm is facing risk that could drive it into bankruptcy and yet the risk occurs every one in a while. At least that kind of company cannot be very long lasting. Numbers that have been putted in the table are estimated on the basis of former theory and interviews. They are estimates and every company has to estimate numbers by themselves.

There are 9 operational risks in this figure. First column contain the operational risk and the next column contain possible effects that it could cause. Third column include the expenses that the risk might cause. Likelihood + expenses column tells the value of the overall impact of the risk with a specific scale. All values have been explained beneath the table.

Table 4. Likelihood +expenses

Risk	Effect	Expenses	Likelihood + expenses
Unstable system	If system is not stable --> makes the work of the employees more difficult--> delays in the processing and payments, employee's well being	Fatigue employees medical expenses --> replacement expenses, delays --> loss of customers and reputational damage	3x2
Mistakes of the people (e.g. Typos)	More clearing work--> other works might be delayed. Mistakes situations where dealing with money	Compensations because of the mistakes --> discounts, or even fines	3x1
Communication	Failed or poor communication --> failed processes --> misunderstood or un received messages --> incorrect work--> internal work more difficult	Additional work --> delays in processing--> discounts or fines	3x1
Regulations	One should closely monitor the development of the regulations, changing regulations --> changes to the processes --> more work	More work --> more human resources --> more expenses	2x2
Human risk	Tasks may be neglected, important person missing--> could affect everybody else's work	Delays in the processing and payments --> discounts to customer or fines to the company	2x1
Terms too open to interpretation	Wrong messages to customers --> litigation --> reputational damage	Court fees, reputational damage--> loss of customers	1x2
Digital innovations (external)	Improvements to information technology --> employees do not know how to use new systems --> delays in the processing and payments --> employee's well being	Employees training costs, delays--> fines --> reputational damage --> loss of customers, fatigue employees medical expenses --> replacement expenses	1x3
Mis-sold products	Wrong messages to customers --> litigation --> reputational damage --> worse, lose license to sell insurances	Court fees, reputational damage--> loss of customers	1x3
Information security	Lose customer data, abuse of the confidential customer data	Reputational damage--> customer losses, fines	1x3

The first risk in the table above is unstable (ICT?) systems. The probability of unstable systems is the highest (3) that risk can get on this scale. It is given a rating of 3 because an unstable system seems to be always present whenever operational risk is mentioned. In addition, every interviewee has mentioned an unstable system and interviewees also mentioned that they have to deal with unstable systems every day. However, determining the costs of unstable systems is much harder to do. Unstable systems can create minor events such as e-mail not working, but can also create devastating errors where the functions of the whole company are interrupted. Because of the large scale of impact, unstable systems were given an expense rating of 2. By contrast, human error was at least as common as an unstable system, but human error is often less expensive. That is why human error received a score of 3+1.

Human error often occurs less than once a week, so the probability of human error has been rated as 2 and the expenses that it could cause are scaled to the lowest measurement. Even the worse kind of expenses caused by human error should not threaten the viability of the company. In addition, terms that are too open to interpretation rarely cause bankruptcy. Usually in the insurance business, contract terms are solid (OR carefully written), but still insurance companies cannot completely avoid situations where customers disagree with the company on how to interpret terms. However, this kind of case only occurs a few times a year in Finland; the related expenses consist of fines or litigation costs.

Digital innovations are common nowadays compared to a decade ago. However, insurance companies do not update their systems every time new technologies appear Digital innovation might cause situations where systems are suddenly out of date. Regularly updating information and terms can be very expensive and it might also create numerous new operational risks. Thus the probability of digital innovation is rated as 1 and the expense is rated as 3. The occurrence of digital innovation may rise in the future and it already seems that companies are struggling with old information technology. In relation, information security is widely discussed in today's financial sector. The financial sector has already witnessed a couple of information security failures, which have caused major financial and reputational losses. Financial organizations do not want to lose further credibility in the eyes of their customers. However, large information security failures are still quite rare in the insurance business, which is why the probability of operational risk caused by failed information technology is rated as 1. But losses can be devastating in the reputational and financial sense; therefore those expenses are rated as 3.

Failed communication is rather a broad area of risk, but at the same time quite clear. All kinds of communication that failed to deliver the message forward are recognized as failed communication. Failed or poor communication occurs in everyday work. Failed communication does not always create direct losses, but do result in wasted time and additional work → probability 3; expenses 1.

Increased regulation is one thing that will affect insurance companies as it has already affected banks. Changes in regulation will have an effect on insurance companies' revenues, if they have not already. Regulators give fines to those insurance companies that failed to follow regulations. Nevertheless, regulatory changes do not happen frequently, even though they are highly topical. Regulations get probability rate of 2 and expenses rate of 2.

Periodically, insurance products have been sold to a customer for the wrong reasons, either accidently or on purpose. These kinds of mis-sold products are almost impossible to control. However mis-sold products, which are presented in this table, are more related to situations where there are a lot of similar products that have been sold for the same reason. In the insurance business it could be that a product that is found to be illegal and all the payments have to be returned to customers. Illegal insurance products result in fines, reputational damage, court fees and even loss of the insurance license. Mis-sold products on a large scale are quite rare in Finland and obviously insurance companies try to avoid mis-selling at any price, because the worst-case scenario could be devastating; like loss of sales rights. The probability of mis-sold products is 1 and expenses that it could cause are 3.

In question number five, employees at Company X were asked how they see identification, calculation and prioritizing of operational risks in Company X. It should be noted that some of the interviewees are working more with operational risks than others, so the answers cover almost all functions in operational risk management. The next figure has been formed on the basis of how operational risks are identified, calculated and prioritized. Figure 11 will show the phases Company X goes through when identifying, calculating and prioritizing operational risks. Identification starts with monitoring operational risks, in which everybody can be involved. For example, an employee who is working in claims services finds out that it is pointless to pass customer-specific information on a single document between business sections, when it can be done satisfactorily once in a week with a single excel report. These kinds of

findings usually facilitate and expedite processes as well as helping to control operational risk. However, operational risks are to be recorded, especially if they are not dealt with, and require resources and actions.

Recorded operational risks have to be looked through and this is where risk owners come into the picture. Risk owners are named persons who report about processes and operational risks to operational risk management. Risk owners report their own operational risks via the Bwise system. Operational risk management then identifies the most important risks, which need more actions or permission from senior management.

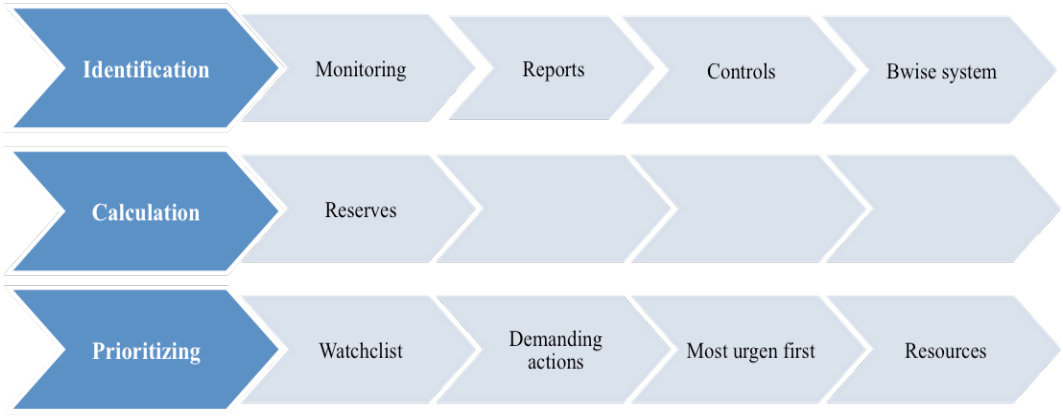

Figure 10. Identification, calculation and prioritizing operational risks.

With tight monitoring and clear reporting the company can save resources and facilitate employees work. In addition, operational risks that have been spotted before they have caused any costs, usually come from the reports that risks owners and operational risk management are working with. Operational risks can also be identified with controls. However, operational risks spotted using controls end up in reports that have been documented in the Bwise systen.

Company X calculates operational risks for reserves. But yet again, the tool that they use is rather simple. One of the operational risks is incorrectly- decisioned claims. It has been estimated to cause a 50 000 € impact to a company; it is also quite likely to happen so the reserve that has to be putted aside is 50 000 €. By contrast, if operational risk management asses that incorrectly-decisioned claims are an unlikely operational risk, the reserve would be only 10 000 €. In one way or another, these reserve calculations are based on historical data and the experience of operational risk management. This is

one section that would need further research in order to get more specific calculations so that reserves would not be too large or too small.

Prioritizing began with watchlists, which posses operational risks that could need further action and specific surveillance. A watchlist is just a tool that helps operational risk management to illustrate the overall picture. A watchlist is also a tool for employees to raise different operational issues. However, operational risks that are on a watchlist still require actions and risk owners or team managers demand these actions from senior management or operational risk management. Everybody wants resources for their risks, which is why they have to justify presicely why their risks need further resources. Nevertheless, internal interviewees thought that Company X should spend more time on operational risk management, because too often operational risks remain at the watchlist level and employees sit back and wait forsomething to happen. Too many operational risks are left without any actions before they become urgent.

Operational risk management decides which operational risks are most urgent and which ones deserve more resources. The most urgent operational risks are usually the ones that are already realized and need rapid reaction in addition to risks that might already have caused damage to the company. The most urgent operational risks are usually allocated additional resources, because the company might suffer losses all the time until the risk has been fixed.

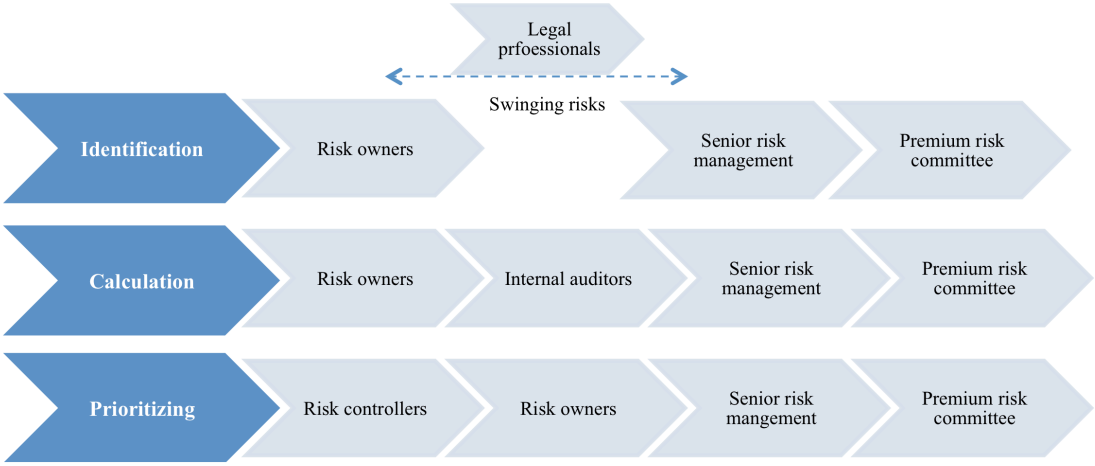

Figure 11. Identification, calculation and prioritizing operational risks.

In identification following monitoring (in which every employee can be involved), risk owners select a few important operational risks to enter into the Bwise system. Then

operational risk managers gather all the risks that risk owners have entered in the operational risk report, which is then presented to senior risk management once a year. However, operational risks might need legal professionals to give their legal opinion. Legal professionals know better for example regulatory demands and therefore they are involved in identification processes. Swinging risks are risks which have been assessed by the risk owners as usual, but senior risk management have sent them back with critical comments after they have evalauted the risks themselves. Risks can swing between these groups until senior risk management finally agree to add them to the company's risk profile. Then the risk profile is agreed by the premium risk committee and the final document is the tool for communication with regulators. Prioritizing is done almost with the same audit trail with one exeption, risk controllers. Control owners are more spread around the organization, which is how different operational risks are managed more specifically and efficiently.

6.2.3 Past, present and future operational risks

The last part of the internal questionnaire deals with past, present and future operational risks as well as mis-sold products and how Company X could have been prepared better for operational risks that occurred. Table 5 gives an overview of question 7 where interviewees mentioned operational risks from the past, present and future. Table 5 shows clearly that the system is present in all three categories. This means that system-related operational risks are the most important operational risks in Company X. System-related operational risks have been raised in almost every question from which we can draw the conclusion that Company X could allocate more resources to systems and IT management. However, systems were not the only operational risk that interviewees raised. In the past there were claims mistakes, which are common in the insurance business. Every insurance company in the world has faced claims mistakes. Some of these mistakes are caused by human error; some of them might be occur because there is something wrong with the insurance terms (reference?). Claim mistakes caused by human error are usually single events and do not cause large expenses for a company, but poor insurance terms might cause multiple false claim decisions. For insurance companies this is obviously a very important area to control, which is how a company avoids additional expenses and reputational damage. Claims mistakes can also result in fines from regulators.

In 2012, regulators decided that men and women should pay the same premiums for their insurance, although the health risks are different between genders (reference). Gender-neutral pricing is a perfect example of regulatory operational risk, which has caused a direct influence on insurance companies' daily operations. Gender-neutral pricing is a relatively new regulatory requirement, so the effects are still quite unknown and would need further research.

Would you mention the order of five or more biggest/most important operational risks regarding your company in the following categories: a) Already realized operational risks b) Currently faced operational risks c) Possible operational risks emerging in the future (numbers next to operational risk is the number of times a particular risk was mentioned by the interviewees)

Table 5. Past, present and future operational risks

Past	
System	6
Letter problems	4
Claims mistakes	2
Gender-neutral pricing	3
Lack of resources	2
Present	
System	9
Letter problems	9
Invoice problems	4
Problems in projects	2
Future	
System	7
Law reforms	5
Political reform	5
Continuity (Partner relationships)	5
Technological development	3

System, letter and invoice problems were all mentioned when interviewees were asked about present operational risks. These are all system-related operational risks and some of them could be visible to customers as well, which might cause customer losses and reputational damage. Answers concerning the system can be explained with today's system-dependent working habits. People work with systems every day and if the systems do not work properly, labor productivity suffers. A poorly functioning system causes minor operational risks every day, which is why system is mentioned in all three categories. System-related risks are clearly the biggest and most important operational risks that Company X has nowadays. Along with the system, interviewees brought up

legal reforms and political reforms when asked about future operational risks. In addition, they expressed their concern about business continuity and technological development.

Legal reforms and political reforms are both regulatory operational risks, which have had a significant impact on the financial sector in recent years. Regulators have taken more responsibility for certain issues, which might affect the security of investors' investments and consumers' insurances. Interviewees believed that this kind of trend is will continue, which is why they specifically mentioned legal reforms and political reforms as one of the biggest operational risks in the future. Regulation as a whole has also been widely discussed in the media following the recent financial crisis. However, interviewees do not consider regulatory risks as present operational risks, which indicate that these kinds of risks have, as yet, no effect on daily actions, but people are still aware of them.

Whether it would be possible to prevent already occurred risks or not, is easy to say afterwards, however the eighth question is about how Company X could have avoided the risks occurred in the past and how Company X could have been better prepared for realized operational risks.

Table 6. Prevention of operational risks

How Company X could have avoided the risks?		How Company X could have been better prepared?
Comedy of errors		Project preparations should be better
Finnish brand should be more involved in IT changes		Better internal project management
Continuity of IT specialist		More resources
Own IT help to Finland		Sufficient testing of IT changes
More efficient processes		More controls/ better controls
System implementations went through too quickly		Keeping key employees
Deficiencies of the system		Recovery management
More IT testing		
Better communication		

As one interviewee said, “this operational risk was a comedy of errors”, which means that this particular operational risk needed a couple of failures before it occurred. Large operational risks usually need a comedy of errors. It was not one button that blew up the nuclear power plant of Chernobyl. It needed numerous system and human errors to happen before disaster was ready. A comedy of errors is hard to avoid, but companies can affect the series of events so that the probabilities of events are reduced.. This can be done with more controls or better processes. However, an institution like a power plant needs to make absolutely certain that it does not leak or explode, where institutions like an insurance company can be exposed more to the risk of a comedy of errors.

More than that, Company X should be more involved in IT changes so that system related operational risks would not occur as a result of bad communication between IT and the Finnish branch. Risks could also have been avoided with better IT testing. Needless to say that IT testing is a vital part of the insurance companies’ daily processes. If the system implementations are rushed through too quickly, it increases almost every time the risks that something goes wrong. Although some of the implementations have to be rushed through quickly, the company should be more aware of other impacts that the implementation might cause. Systems are often quite fragile, which means that corrections, for example to invoicing, might have an impact on other system properties. This kind of lack of awareness is due to the fact that IT specialists do not necessary have the sufficient level of knowledge about processes in Finland so repair decisions do not take into account all relevant angles. Taking this into account Company X should have its own IT specialist to ensure better continuity.

A large part of the functioning of the system is communication. If the communication between people and departments is limited and poor, it significantly affects the operations of the company. Poor communication between operations and the IT specialist weaken the functionality of the system. The better the picture of the practices the encoder has, the easier it is to make the right corrections the first time, without any complications.

However, every company faces problems every now and then, which is why preparations for operational risks are important. Interviewees mentioned a few ways that Company X could have been better prepared better for the operational risks that it has faced. Project preparations should have been organized better. Management should select people more carefully for projects and the people who have been selected should

plan more carefully the steps and the progression of the project. These are two easy tasks that can be done at the beginning of the project. In addition, operations almost always need more resources, however in this current economic situation resources are hard to come by and therefore additional resources are not usually allocated.

Nevertheless, controls are a great way to improve preparedness for operational risks. Operations should focus deeply on controls that would facilitate the working environment. Controls cannot be too rigid, because this may cause delays and frustration among employees. An excessively rigid working environment may hamper the retention of key employees because annoying and inconvenient practices and policies could have an effect on the working atmosphere. It is vital to maintain a positive working atmosphere if a company wants to keep key employees. The retention of key employees is very important to a company like Company X because the education and training of a new employee is quite slow and expensive. Also, more experienced employees can operate much faster and provide a more professional touch. More experienced employees can take more responsibility and develop new or better controls and policies.

However, interviewees all agreed that Company X should have more organized and better recovery management. Recovery management is highly important when operational risk arises. A company that is exposed to operational risks should be prepared to manage different kinds of areas of operational risk, of which reputational and regulatory are very important. This is because these risks might have large tail losses and could easily be forgotten. If a company does not manage reputational risk properly it could cause customer and financial losses. In addition, regulatory risks should be dealt with immediately in order to avoid fines. If recovery management is at an inadequate level in a company, the consequences might be fatal.

The last question introduced here is about interviewees' previous job and how operational risks were different there. Employees that were interviewed have been working at Company X for a while now, which had an effect on answers to question 10. Some of the interviewees could not mention any operational risks from the previous job. That is, question number 10 (How do operational risks differ between Company X and your previous workplace?) did not bring any additional value to this study, which is why it has been left little attention. Why was it much harder to talk about operational risks from previous jobs? There could be multiple reasons for this, for example, employees do not remember, or there is no previous workplace, but the actual reason

could be that operational risk, as a risk category, is rather new. Therefore, it was quite impossible to mention any operational risks from the past because 10 years ago operational risk was a relatively uncommon concept.

6.3 External Questionnaire

In this chapter the answers from the external questionnaire are presented. Five people outside Company X have been interviewed and every one of these people is a professional operational risk manager who deals daily with operational risks. They are from are other insurance companies in Finland. These insurance companies are different from Company X in many ways, actually one of them is a global banking group which will give a little a bit perspective to this section. Two of them are Mutual Pension Insurance Companies, which means that they have to obey different regulations and legislation. They have similar and different operational risks than other insurance companies. One of provides retail and commercial banking services as well as insurance services. Last Insurance Company offers general insurance such as motor vehicle insurance or house insurance.

In this chapter the answers from the external questionnaire are presented. Questions are not always presented in the same order as they were asked in the questionnaire. This is because some questions are related to others and the related questions are presented consecutively in order to facilitate understanding of the connections between questions. The answers are presented in different figures and tables, the same as in the internal questionnaire chapter. This is because it is clearer to compare the answers in the next chapter. It is also easier for the reader to understand the similarities and differences between the internal and external questionnaires. This chapter starts with the already familiar four-field matrices and continues then to the interpretation of other answers.

All the four-field matrices below are formed with the answers of question 2 so that size of the figure depends on how many people have brought it up and the location of the figure depends on which category it is suitable for. For example, system breakdown is the biggest figure and it belongs to systems. However, if some of the topics fit in both system and people, or processes and system etc. it goes between those fields, depending on which has the stronger influence.
The first matrix from the external answers includes all kinds of operational risks around the world. With just a quick look it can be said, unlike in the internal questionnaire,

there are more answers that go into the field of regulation and external risk. Also more minor risks do not get too much attention here. It can be explained by the respondents' job assignments. External interviewees were professional in the field of operational risk management. This means that they may have a wider picture of operational risks and therefore the answers show some differences as well.

Nevertheless, in the first external matrix, regulation and external risks, system and people get attention when processes are left more untouched. Of course the ellipses can be placed almost everywhere depending on the point of view. However these ellipses have been located from the perspective of the interviewees. The answers to question 2 are diverse and only three answers earned two references. These three answers were system breakdown, VR (State-owned Railway Company in Finland) system implementation and rogue traders. System breakdown is easily located in the system, but system implementations include more than just system caused operational risks. There is usually a lot of planning and testing before implementation. If testing, for example, has been insufficient the implementation could be devastating for a company. System implementation is also sensitive to human error. For this reason VR system implementation is closer to the people field than system breakdown. By contrast, rogue traders have been located in the people field close to regulation and external risks and processes. Rogue trader is more than just the greed of one person. There has to be deficiencies in controls and processes to make it even possible. In addition, there are often problems with regulatory compliance. There has to be opportunity but in the end it is a person who commits the abuse.

There were a couple of other answers related to regulatory compliance, such as the Libor scandal where a handful of the biggest banks in the world manipulated the interbank lending rates. UBS is one of the banks involved in the Libor scandal. UBS got unpleasant publicity also when a rogue trader from the bank was caught. Controls and processes failed twice in a short time at UBS. EU regulators fined JP Morgan for involvement in the Libor scandal. JP Morgan's fines were 72 million Euros while UBS' fines were 12.7 million Euros. Société Générale was also involved in the Libor scandal. These banks did not follow regulations, but processes and controls failed also. With controls, companies try to, for example, prevent opportunities where an employee could abuse their position. Especially when the economy is in recession, the financial pressure people are under can grow unbearable, which can lead to abuse. Of course controls have other functions as well. With controls a company tries to prevent human error.. Controls work also for processes and the support structure.

Under the second question it can be said that external interviewees think that operational risks caused by regulations or regulatory compliance should be under the supervision of the company. Operational risks caused by people were also raised in the second question. Operational risks caused by project management or operations against regulations are located in the people field. For the success of the project it is highly important to select the right people to manage the project. If a company fails to choose competent management for a single project, multiple operational risks could occur. With bad management, the schedule of the project could be delayed, which means lost working hours. Lost working hours can be transferred straight to lost money. However, if the project fails to achieve the desired result it would be an even worse scenario. This kind of situation could be avoided with proper project management selection procedures.

As well as project management, the operations against regulations are mainly due to human actions. People can try to make profits by intentionally violating rules of regulators. This kind of abuse is prevented with controls, but not all controls apply when the abuser is on senior management level. However, abuse committed by intentionally is quite rare. More often, regulations are broken when a company fails to monitor changes in regulations. Nowadays regulations change more often than a decade ago, so companies must devote more resources to monitoring different regulators. An internationally operating European company may have to follow regulations at the local level, at the country level and regulations from the EU and the USA. Operations contrary to regulations are usually “rewarded” with fines from the regulators. Large fines are often reported in the media, leading to reputational damage. As it can be seen from the matrix above, one of the ellipses is in the middle of the fields. Reputational damage is an operational risk that can be caused by any of the four fields in the matrix. Processes are left quite alone and the only one is “problems in processes”. Although it is left alone it does not mean that it is not important. Actually processes are often involved when talking about controls and therefore it will be discussed further in this

The list above is formed from the answers of the interviewees in question 2. Answers have been put in the four-field matrix so that the bigger the ellipse the more references it has received. Also the location of an ellipse depends on which category it belongs to most.

1. System breakdown
2. VR system implementation
3. Rogue traders
4. System implementations
5. Hacking
6. Compliance of the procedures
7. Project management
8. Problems in processes
9. Operations against regulations
10. Libor scandal
11. Société Géneralé
12. UBS
13. J&P Morgan fines
14. Deepwater Horizon oil spill
15. Blackout
16. Eläke Tapiola mess
17. Reputational damage

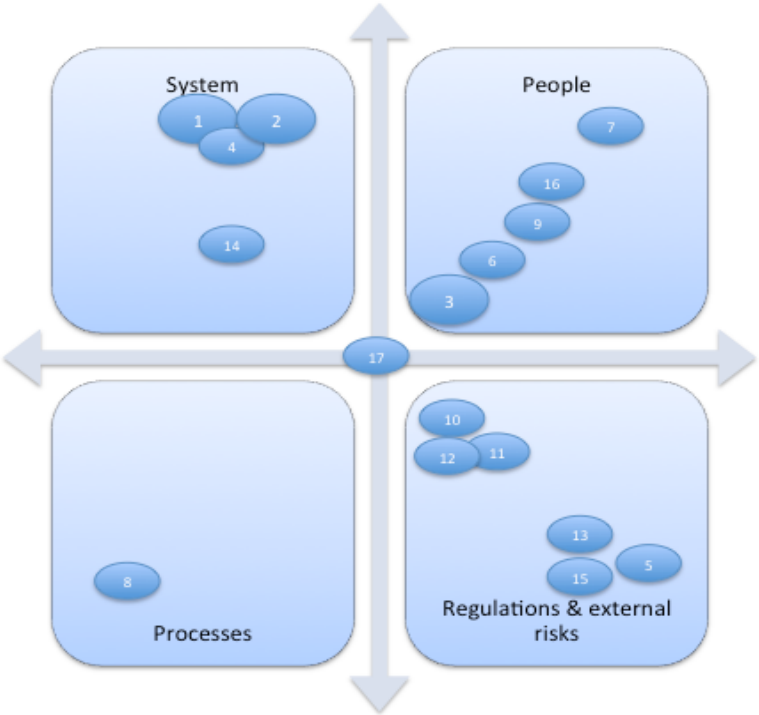

Figure 12. Would you mention a few realized operational risks that have occurred in Finland or worldwide?

After general operational risks, the interviewees were asked about operational risks in their own companies. In the third question interviewees mentioned 26 different operational risks, which are more or less part of companies risk identifications. Again, functioning of the systems was raised more than once. The three most mentioned operational risks were old systems, system breakdown and typographical errors (Typos) all mentioned three times. In addition, risks that were mentioned two times were data

run crashes, system implementations, information security, communication, functionality of the processes and agreement practices.

The list above is formed from the answers of the interviewees in question 3. Answers have been put in the four-field matrix so that the bigger the ellipse the more references it has received. Also the location of an ellipse depends on which category it belongs to most.

1. Old systems
2. System breakdown
3. Typos
4. Data run crashes
5. System implementations
6. Information security
7. Communication
8. Functionality of the processes
9. Agreement practices
10. E-mail does not work
11. Phishing messages
12. Know-how
13. Actuaries calculations
14. Phone service
15. Insuring mistakes
16. Project risks
17. Quality of the data
18. Partner risk
19. Statutory customers
20. Reputational damage
21. Media
22. Following the regulations
23. Local authorities
24. Money laundering
25. Terrorism regulations
26. Legislation

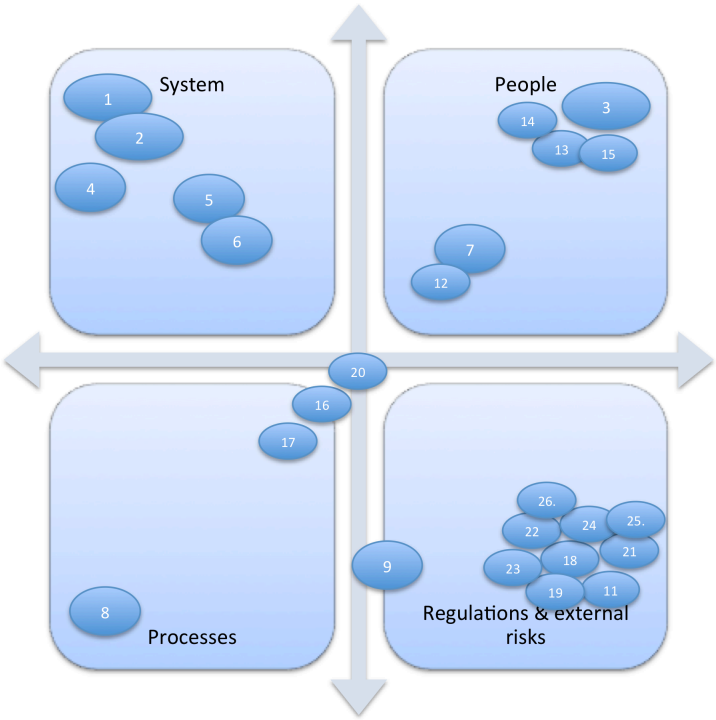

Figure 13. What kind of daily operational risks your company face?

From the nine most mentioned risks five are located in the system field, this indicates that firms are forced to update their old and weak systems. When firms are renew their information technology, new operational risks usually occur. If old and new systems do not communicate well enough, it could cause data losses, failures in information security, data run crashes and even system breakdowns. Nowadays, many firms struggle with fast developing information technology so it is not surprising that operational risks related to systems were mentioned often in the questionnaire.

Along with system, the people field got multiple answers from interviewees. Risks caused by human actions are quite typical operational risks. For example, typos (typographical errors) are always present when people are working with computers or other devices. A classic example of a typo could be when an employee accidentally types the wrong account number and payments vanish somewhere they should not go. Controls are the best way to try to avoid typos. System which send warning message to the computer screen when numbers are wrong, is a basic control to avoid typos. Even controls cannot completely eliminate the risks of typos, but controls should at least expose mistakes before they cause irreversible consequences. The second biggest ellipse in the people field is communication. Although communication is located in the people field it is linked to system and processes. Bad communication is usually people's faults, but sometimes, poor processes or incapable systems do not suit reasonable communication. For this reason communication slides towards processes and system, but still stays in the people field.

Other operational risks in the people section would be know-how, actuaries' calculations, phone service mistakes and insuring mistakes. Employees' know-how firmly depends on the level of training that the firm offers, but also hiring the right people to do the job is important. Sometimes it is quite hard to find the perfect employee, especially when a new employee is replacing a former one. Let's image a situation where a Norwegian employee leaves a Finnish company and the empty place has to be filled in a month so that delays remain manageable. A requirement for the job is that the candidate has to speak Norwegian. There is a limited number of Norwegians living in Finland, not to mention that someone would be available for hire and qualified for the job. Now in the first place the company faces a human risk because the replacement is difficult to find. Secondly, because of the language requirement, there are a limited number of candidates, which could lead to the hiring of an unqualified person.

As we can see, ellipses have formed a cluster in the regulations and external risks field. All of the risks in the cluster are on an equal position. Phishing, partner risk and media are external risks and controlling them is quite hard because they have their own interests. Phishing can be controlled through proper communication with customers. This kind of activity has not been a matter of concern for insurance companies so far. For example, banks' customers receive phishing messages every once in a while when someone is trying to acquire account information and passwords. Banks inform customers how to react when facing phishing messages, but in the end it is the responsibility of the customer to recognize fake messages. However, operational risks caused by partners and the media are more significant to an insurance company than phishing messages. Partners are vital for insurance companies like Company X. Company X partners in Finland, banks, sell Company X's products to end customers. Needless to say, partners are vital to every company, but some partners are easier to replace than others. Mutual pension insurance companies need partners to transfer information between mutual pension insurance companies. Every Finnish citizen has their salary information in the possession of the company, which operates between different pension insurance companies, for example, exchanging information between the companies. Mutual pension insurance companies have a special relationship with the media. That is, Finnish people have to pay a pension payment from their salary. So these companies have a statutory position and therefore they are under the scrutiny of the media. It is very hard to control the media as if it were just another operational risk. The media works independently and can create reputational damage to a company if necessary. Controlling the media is not impossible. Working with the media is better than trying to avoid it as much as possible. The cluster also includes ellipses that are strongly related to regulations.

External interviewees raised different kinds of operational risks that follow regulations: Statutory customers for mutual pension insurance companies, money laundering, terrorist regulations, local authorities, legislation and following the regulations in general for all insurance companies. Statutory customers mean that mutual pension insurance companies have to accept every one as their customer if asked, because of the legislation in Finland. As mentioned before, the most harm from regulations and local authorities, along with legislation, is that companies have to be constantly aware of the changes in regulations and legislation. If a company is not aware of some regulation it could lead to compliance issues, which can lead to fines and reputational damage. Following the regulations has increased continuously. One of the major problems in regulations is that there are multiple parties which publish regulations. For example

Local authorities, EU, BIS and EBA all release their own regulations. Regulators do not always communicate with each other, this creates more complications. It would be desirable that regulators communicate better with each other. Global regulators take money-laundering and terrorism regulations very seriously nowadays. Companies are strictly prohibited from involvement in money laundering or financing terrorists or criminals. That is, companies have to know their customers more specifically than before, which means more resources. Also, more regulations might increase the risk of accidently creating operations against regulations.

The list above is formed from the answers of the interviewees in question 11. Answers have been putted in to the four-fielded matrix so that the bigger ellipse the more references it has received. Also the location of an ellipse depends on which category it belongs most.

1. Reputational damage
2. System implementations
3. Technical issue
4. Delays in payments
5. Exxon Valdez
6. Chernobyl
7. Bankruptcies 2008
8. Apathy to follow regulations
9. Money laundering
10. Terrorism regulations

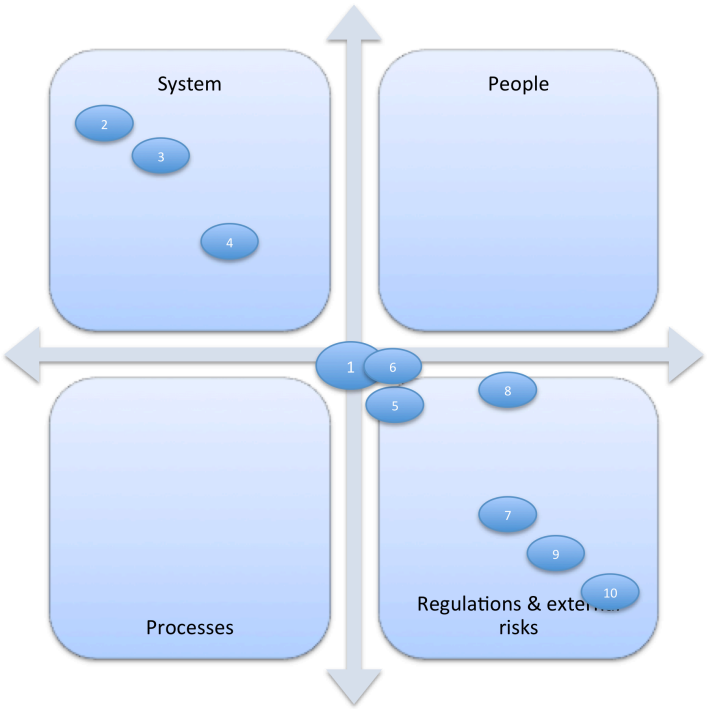

Figure 14. What is, in your opinion, the single largest realized operational risk?

The last four-field matrix has been formed from the question where interviewees discussed the biggest operational risks that have occurred in the world. The question did not specify “the biggest” in any particularly area. Reputational damage was the only risk that received more than one answer and it is located in the middle of the matrix as before. There are three single events that have created major catastrophic consequences. On 26 April 1986 a nuclear power plant started to burn and finally exploded in Chernobyl, Ukraine. The Chernobyl disaster was caused by multiple operational risks that occurred at the same time. There were failures of the systems; the processes weren’t followed correctly, employees were fatigued and made mistakes, and the regulations were not followed either. Failure in all four categories caused the world’s biggest nuclear power plant accident. The Exxon Valdez oil tanker disaster was the result of a fatigued employee, apathy in following regulations, poor processes and system failure. Both these disasters needed more than one realized operational risk to take place before the final push could happen. For example let’s image that the Chernobyl power plant needed 6 operational risks to occur in a row before meltdown. In addition, if we think, for example, that the average probability that one of the six risks occurs was 3 %. This means that the probability of meltdown was 0,03^6 = 0,000.000.000.729. However today there could be 20 occurred operational risks before meltdown of a nuclear power plant. These kinds of disasters are always a sum of many improbable coincidences. Apathy following regulations was one of the main reasons for the bankruptcies in 2008 and for that it has been located in the regulations and external risks field.

Regulations have many purposes and one is to prevent disasters from happening. Others are to prevent money laundering and financing terrorist or criminals. Interviewees, when asked the biggest operational risks in the world, answered money laundering and terrorism regulations. Financial institutions must know their customers well enough so they do not operate with terrorists or criminals and they cannot be part of money laundering either. These two operational risks have been located in the field of regulations and external risks. Regulations forbid both actions but if a company fails to know their customer, they could finance terrorism without knowing it. It is the responsibility of financial companies not to be involved in anything like that. For insurance companies, money laundering brings more challenges because criminals favor insurance frauds. Regulations for insurance companies are tightening all the time, which brings even more challenges. The last three ellipses (2, 3, and 4) have been located in system. System implementations seem to have generated problems for multiple companies around Finland. Along with system implementations, technical issues have caused large operational risks in the financial sector and, as stated earlier, one reason for

this could be rapidly changing and developing information technology which companies are trying to keep up with.

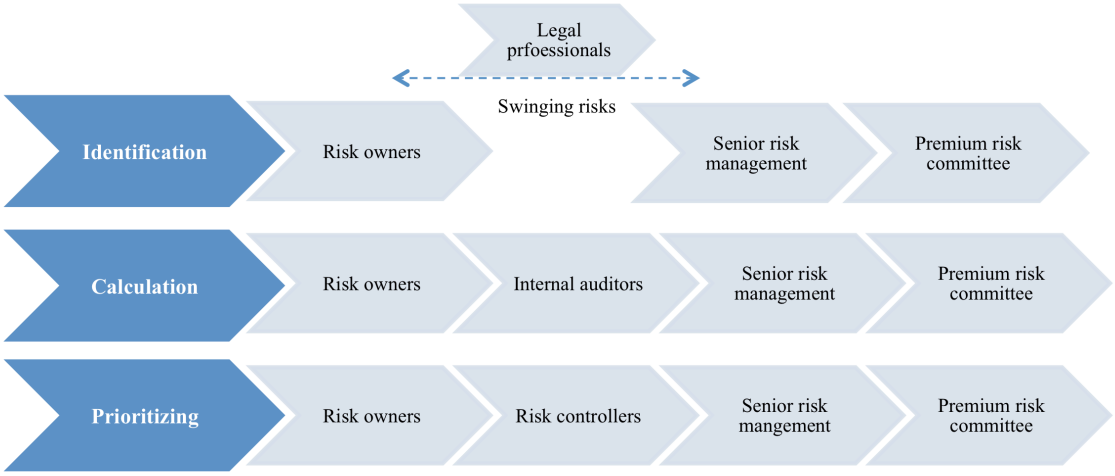

Figure 15. Identification, calculation and prioritizing operational risks.

Operational risk management is a very topical and developing area of risk management and therefore interviewees were asked about the resources that they have available for operational risk management. Interviewees reported how many people, how much time and money they have for operational risk management. The next figure gathers all the answers in a single table as a summary.

Summarized answers to question: How many resources does your company have available for operational risks?

People	Time	Money
-Usually one or two people responsible along with a small team 5-15 people. -In addition, operational risk management is happening alongside the daily work of all employees..	-Risk management working daily with operational risks. -In addition, few times per year going through and reporting all operational risks.	-Money goes to the maintenance of processes, reporting system and its development. -Exact amount of money spent on operational risk management is difficult to determine because of the broadness of operational risk management. -Large and developing area and there for more resources spend.

Figure 16. Operational risk resources.

Every company has at least one full-time risk manager responsible for operational risk management. Along with the risk manager there are 5-15 people in the risk management function. Usually this risk management function deals with other risks not only operational risks. A risk management function for operational risks only is still quite rare. However, the supervision of operational risks has been delegated to a wide range of different business functions and every employee is responsible to report realized operational risks to risk management.

The time that insurance companies use to manage operational risks is limited. Risk management works daily with operational risks, but they deal with other risks also. In addition, there are meetings a few times per year where risk management gathers all operational risk data. Risk management analyses this data and produce a report where the biggest operational risks are brought to the attention of the board of directors, who then make a decision on the basis of the report. Interviewees were not able to give a precise number for the money spent on operational risk management, not because it is confidential information but because the exact amount is difficult to determine due to the broadness of operational risk management. Operational risk management usually uses money for maintenance of processes, reporting, systems and their development. The next figure focuses on how insurance companies identify, calculate and prioritize operational risks in general.

Summarized answers of question: What kind of tools your company uses in following categories: a) identifying b) calculation c) prioritizing of operational risks.

Identification	Calculation	Prioritizing
-Realized operational risks are reported in the system. -Every function defines operational risks. Yearly risk mapping/reports.	-Calculation is still rather difficult, which is why insurance companies rarely use special formulas for operational risks → no Euros per risk. -Some define operational risks probability and effect from one to five scales. Reserves. Capital adequacy 01.01.2016	-Person responsible raises a few important risks up and prioritization is done in the board of directors with recommendations from risk managers. -Usually only biggest decisions go to board of directors.

Figure 17. Operational risk tools

Finnish insurance companies have begun to collect historical data from realized operational risks. With historical data they can prepare better for operational risks in the future. Interviewees said that they use the system to report all realized operational risks. Every function is responsible for reporting their own realized operational risks in the system. Operational risk management then organizes yearly mapping where they raise the most important risks with the board of directors. Some insurance companies monitor key risk indicators through the year which gives them the ability to improve reaction time. Although gathering operational risk data has shown even large improvements, calculations from this data are still rather difficult so companies rarely use any calculation methods to support operational risk management.

Likelihood	Consequences				
	Insignificant (<1tEUR)	Minor (1-10tEUR)	Moderate (10-100tEUR)	Major (100t-1mnEUR)	Catastrophic (>1mnEUR)
Very Likely (>30%)	High	High	Extreme	Extreme	Extreme
Likely (10-30%)	Moderate	High	High	Extreme	Extreme
Moderate (5-10%)	Low	Moderate	High	Extreme	Extreme
Unlikely (1-5%)	Low	Low	Moderate	High	Extreme
Rare (<1%)	Low	Low	Moderate	High	High

Figure 18. Likelihood and Consequences matrix

New regulations from Solvency 2 might oblige insurance companies to calculate certain operational risks and, because of this, some Finnish insurance companies are already using standard models to support operational risk management. Some companies scale

operational risks on the basis of probability and impact. This model gives values to the probability and impact of certain operational risks. Usually probability and impact have been rated on a scale of one to five so that one is low probability/impact and five is high probability/impact. These numbers are multiplied by each other and the final effects captured. The figure above should clarify how the model works.

Companies use this model to prioritize their operational risks. Risks that have a value of 25 are the most important risks and companies should focus on managing those risks. However, the biggest risks that need large changes or actions are usually raised with the board of directors. The board of directors then makes decisions with recommendations from operational risk managers. Risk managers prioritize smaller risks after they have analysed operational risks data that the company has collected.

Both tools and resources are linked substantially to the regulations of operational risks. That is, regulators might give new tools to manage operational risks and new tools to measure operational risks. Regulators will also create new regulations that might induce requirements, which lead to more resources spent. Interviewees mentioned often that new regulations could create more costs. This is because regulators might require that companies have to know their customers better, companies have to collect more operational risk data or companies just have to follow regulators very closely so that there will be no surprises. The sixth question for external interviewees was: Do the regulations of operational risks have an effect on your business? How? The next figure will present a summary of the answers categorized in four main regulators: Basel 2/3, Solvency 2, Finnish law/regulators (FIVA) and EU law/regulators.

Basel 2	Solvency 2
-Gave a lot of standards and methods to operational risk management, which later "spilled" on the entire financial sector, although Basel 2 is for banking sector only. -Regulations do not make it more difficult, although it is difficult to keep up with changes.	-Will not concern mutual pension insurance companies (MPIC), but Solvency 2 includes a lot of things which are reasonable and which connect to reliable corporate governance. -Solvency 2 has been under monitoring a long time.
Finnish law/regulation	**EU law/regulations**
-Legislation for mutual pension insurance companies is currently being renewed. -Attention towards operational risks is, however, growing all the time. In Finland such an intermediate step where the Financial Supervisory Authority (FIVA) demands an annual report for losses comes before Solvency 2. Might create problems if collected data is not valid.	-Implementation of operational risk regulation from EU to systems is operational risk. -Regulations may be surprises and reaction time might be short. This requires a lot of active monitoring, rapid actions and resources.

Figure 19. Regulations

The job of the regulators is to give standards and methods to companies so that they could offer investors and customers reliable and stable services. Regulators also want to increase companies' transparency in order to earn the trust of investors and customers. A high-level regulatory framework makes it easier for running errands, giving continuity and knowledge. As we can see from the figure above, there are multiple regulators that have an impact on insurance companies in Finland. According to interviewees, the hardest part is to follow the development of regulations and what makes it even harder is that there are many regulatory entities. One problem is that these entities do not always communicate with each other so there might emerge conflict between different regulations. This is one reason why insurance companies have to follow every regulator closely. Companies wish that regulators would communicate better with each other so that the coordination between them would be improved.

Interviewees mentioned that regulations do not make operational risk management more difficult, but new regulations might affect resources spent on operational risk

management. Some of the insurance companies in Finland have included regulatory guidelines from the beginning and that is why there should be no surprises in the future. Nevertheless, the implementation of operational risk regulation from the EU in systems is an operational risk. Regulations may still be surprises and reaction time might be short. This requires a lot of active monitoring, rapid actions and resources. Although Basel 2 regulations are for banks it also concerns insurance companies in Finland. The Financial Supervisory Authority (FIVA) has taken operational risk management areas under their standards therefore insurance companies are under some regulations from Basel 2. Solvency 2 is a similar regulatory authority to Basel 2 but it is for insurance companies and not as developed as Basel 2. Solvency 2 will not concern mutual pension insurance companies (MPIC) but will include a lot of reasonable issues connected to reliable corporate governance. In addition, the capital adequacy reform will be different to MPIC's due to the fact that dividends are not paid. The capital adequacy reform is going to Finnish parliament in 2015. While a lot of work has been done with Solvency 2, it is still mostly monitoring insurance companies. Solvency 2 is a rather smaller regulator compared to Basel 2 & 3.

As stated earlier, legislation for MPIC's is currently being renewed, possibly resulting in demands for operational risk management. However, demands should not have an impact on daily processes, but attention towards operational risks is growing all the time. Non-life insurance companies will receive new regulations and guidelines in 2015-2016, which include reporting and classification methods at least. In Finland, an intermediate step where FIVA demands the annual report of losses comes before Solvency 2. This might create problems if collected data is not valid. However, insurance companies in Finland seem to have collected data sufficiently so far. Regulators may demand technological development as well and that is one reason that interviewees were asked about technological development. Technological development is not only a technological issue, but also a matter of opinion because of everyone's online activity. People's actions have been taken into account when renewing information technology. Companies have to inform customers continuously, but in the end companies cannot be responsible for every click that customer execute. Let's create an example of harmful customer online action. The Internet is full of phishing messages which should be ignored immediately. Nevertheless, there is always somebody that accidently gives his/her personal information to thieves. The only action that a company could do against this kind of fraud is to inform customers but after this it is the responsible of the customer to notice if someone is trying to get his/her personal information. The ninth question asked was: How great a risk/threat is the development

of technology and your company's constantly growing dependence on it? Figure X below presents the answers. There are three ellipses, which are opportunities, risks and actions. Many of the interviewees think that technological development is a combination of opportunities and risks. They also suggested some actions, which could be taken to decrease the risks that technological development creates.

Interviewees believe that technological development removes certain risks such as typos and other kinds of risks caused by human error. In this respect more controls could be installed to facilitate supervision. In addition, data collection becomes easier because data becomes more centralized. On the other hand, centralized data pose a more severe hacking risk. Interviewees all agreed that dependence on the technology is huge and will not decrease in the future. Interviewees also brought up the point that technological development could cause new kind of risks that are still unknown. Technological development is a business risk that creates operational risks. If a company does not keep up with technological development it cannot provide customers with proper digital services, which may lead to customer losses. Keeping up with technological development is actually a mandatory requirement in the current, competitive, economic environment.

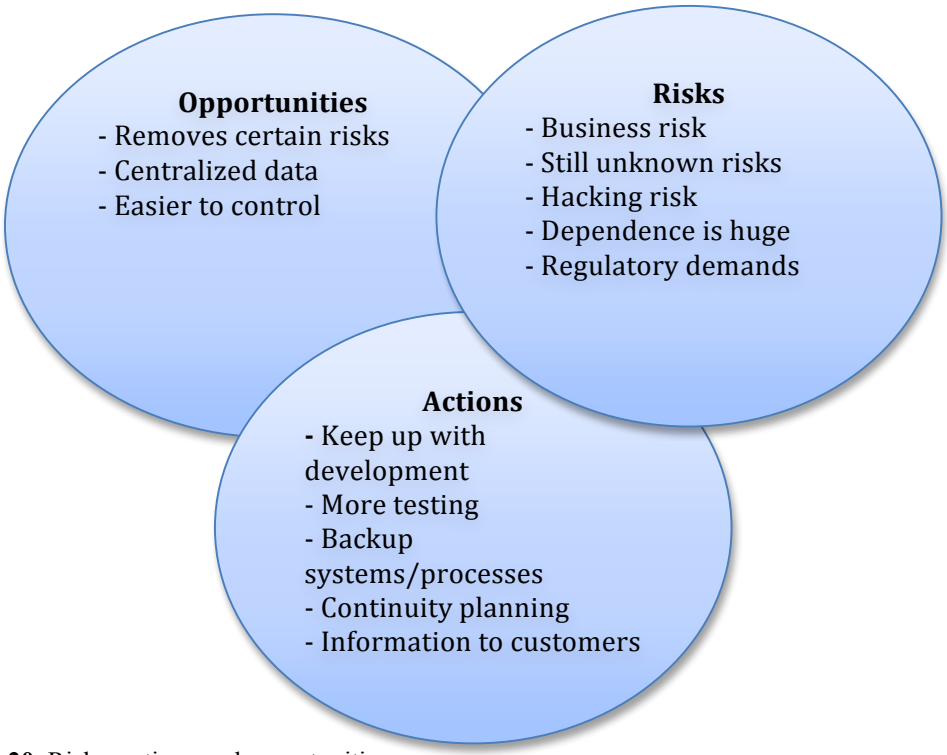

Figure 20. Risks, actions and opportunities

What actions then could be done to manage these risks? As I have said before, companies have to keep up with development in order to maintain competitive force. To do this, companies have to make sure that technology is updated as often as necessary. When updating the system it is very important to run enough tests so that incomplete changes do not go online too early. Also backup systems and processes have to be in shape. If there is, for example, a black out, management has to make sure that there are no major interruptions in functions. In addition, there have to be processes for this kind of situations. Both backup systems and processes are strongly related to continuity planning. Operations of the main functions have to be ensured even in exceptional circumstances. System crashes should not cause a long period of malfunction. Continuity planning also involves contracts with business partners. Some contracts are vital to companies so contracts should be longer than one or two years. Companies have to develop and monitor technology continuously, which is why they have to pay attention to it in now and in the future.

The next figure will show the answers to the question about operational risks in the past, present and future. Operational risks that received two or more answers are presented in the figure below. Four out of five interviewees raised reputational risks when asked about past realized operational risks. Reputational risks include all kinds of events that have caused reputational damages, such as fines or customer service malfunction. Fines and customer service malfunction might cause negative publicity which can cause customer and financial losses. Needless to say, insurance companies do not want negative publicity and that why they need a good relationship with the media. In Finland the best way to earn confidence is through transparency. MPIC's in particular, are under the supervision of Finnish people and media because they control the pension funds of Finnish people. One problem with the media is that they do not always investigate thoroughly before releasing news. For example, a couple years ago a reputable newspaper released news including accusations against one insurance company. Although this news was not true, the insurance company had to prove it to the people. Investigations caused costs to the company although the accusations were incorrect.

Reputational damage was also raised in present operational risks, which is not a surprise because insurance companies are continuously under the influence of reputational risks. The biggest difference between past operational risks and present operational risks were regulations. Regulations were hardly mentioned in past operational risks, on the other hand regulations were the most mentioned topic in present operational risks. Overall

regulations were mentioned four times, money laundering 2 times, financing terrorism 2 times and following regulatory changes 2 times. Regulations are clearly a large part of operational risk management in today's insurance companies. Regulators might demand different reports and different methods than companies are now using. That would cause more costs. Regulators have also tightened regulations for insurance companies concerning financing terrorism and money laundering. Insurance companies have to know their customers better so that they do not accidently, or intentionally, participate in money laundering or financing terrorism. Regulations about knowing your customers and other regulatory changes require more resources from companies. Regulatory demands create compliance risk as well, which is a large operational risk for insurance companies.

Would you mention the order of five or more biggest/most important operational risks regarding your company in the following categories: a) Already realized operational risks b) Currently faced operational risks c) Possible operational risks emerging in the future (numbers next to operational risk is the number of how many times a particular risk was mentioned by the interviewees)

Table 7. Past, present and future operational risks

Past	
Reputational damage	4
Negative publicity	3
Media	3
System crashes	3
It outsourcing	2
Fines	2
Present	
Regulations	4
Knowing your customer -->Money laundering	2
Financing terrorist	2
Changes in regulations	2
Reputational damage	2
Cyber security	2
System implementation	2
Future	
Securing sensitive information	3
Vulnerability of the information environment	2
Regulations	2
Cyber risks	2
Risks that haven't occurred yet (emerging risks)	2

Two interviewees said that cyber security is one of the present operational risks for their company. This is related to compliance risks because companies might get fines if customer data is abused. This means that companies have to ensure that sensitive customer data will remain confidential and confidentiality is essential to insurance companies. Securing sensitive information is also a future operational risk that concerned interviewees. Furthermore, the vulnerability of the information environment is one of the future operational risks according to interviewees. Hacking of sensitive information has increased in the recent past and it could spread to insurance companies in the same way it has spread to the banking sector. There were also mentions of some operational risks that have not occurred yet. For example if radiation from mobile phones was found to be harmful to health, it could cause major losses to insurance companies. Insurance companies would have to pay a lot of compensations and finally reprise their products.

Would you mention some operational risks, which can be devastating in the future?

SYSTEM		**PROCESSES**	
Cyber risks	Information technology	Continuity	Working in exceptional circumstances
PEOPLE		**EXTERNAL RISKS**	
Communication between IT and management		Climate change	Cyber risks
Modelling errors		Hacking	Inventions
Human risk (Staff shortage)		Unexpected major cause of sickness (asbestos)	Pandemic
		Recognition of the existence of the field	

Figure 21. Devastating operational risks

Interviewees were also asked about operational risks that might be devastating in the future, not to their company but in general. In the figure below there are four already familiar categories in which the answers have been located. Cyber risks are the only operational risks that have located in two categories, system and regulations and external risks. This is because cyber risks can be external or internal risks and the

functionality as well as protection of the system affects the likelihood and impact of cyber risks. Every other category possesses the same operational risks that have been mentioned before in this study but regulations have been omitted from the answers. This might be due to the fact that insurance companies do not see regulations or regulatory changes as an operational risk that could be devastating to a company. Nevertheless, above we can see operational risks that might cause trouble for insurance companies in the future.

7. INTERPRETATION OF INFORMATION FROM CASE STUDY

Now that we have gone through internal and external questionnaires it is time to focus on differences and similarities of the answers. As you may have already noticed that there were mutual understandings between internal and external interviewees as well as there were disagreements. Previous literature concluded that operational risk management is rather new and rising risk category. This announcement was surely accepted among the interviewees. Companies have become to spend more resources to operational risk management, which indicate that companies have begun to slowly appreciate more operational risk management in the last decade. Companies have understood that they have to manage not only credit and market risks but also operational risks. In addition the regulators have paid more attention to operational risks as well, which is one reason that companies have to reallocate resources to operational risk management. Information for this chapter is mainly collected from the interpretation from questionnaires. This chapter will give good references to further studies.

Chapter 8.1 provides a summary of the answers from the questionnaires. Chapter 8.1 will also provide main differences and similarities between internal and external questionnaire. Chapter 8.2 answers to the research questions. The key operational risks and most common tools used in Finnish insurance companies will be presented on the base of the answers of the interviewees. In addition how insurance companies in Finland prioritize their resources to operational risk management.

7.1 Replies of the Questionnaires, Main Findings

Both internal and external interviewees named numerous system-elated operational risks that have occurred in companies around the world. This tells us that financial companies have faced system-related operational risks and those realized risks have caused enough losses that they have become public. The biggest differences were in operational risks caused by people as well as regulations and external events. External interviewees mentioned more operational risks that were caused by human error or other human actions. However, this does not tell us much because these answers were about operational risks from companies around the world and, as mentioned before, external interviewees work daily with operational risks and therefore can be expected to

observe operational risks more specifically. Operational risks mentioned by external interviewees might be closer to financial companies and, it can be also seen from the answers, on this basis, financial companies faces more operational risks caused by people, and regulations and external events, than other operational risks. However, the second four-field matrices tell us more about operational risks that Finnish insurance companies are facing today, which is more important regarding this study.

The second matrices are much more interesting because they deal with operational risks from interviewees' own companies. It can be said that they posses some of the key operational risks which occur in Finnish insurance companies. Firstly, both internal and external interviewees were able to mention much more single operational risks when asked about their own company. The main operational risks in Company X seem to focus on system and people, when other Finnish insurance companies clearly added regulations. However, interviewees' positions in the organization have to be taken into consideration. Operational risks seem to be different depending on the employee's position. For example, a claims associate who is processing customer compensation cannot work for an hour because the system is down. This can be very frustrating and it will slow down processing. In contrast, an operational risk manager does not consider that this kind of system malfunction is very serious because the operational risk manager considers the matter on a large scale. Losses from this kind of situation are usually minimal and hardly calculable, which is why operational risk managers are not necessary interested in it. Of course, if system malfunction is a daily problem, the risk manager should be interested in it. Nevertheless, external and internal interviewees stress the importance of system-related operational risks, which means that regardless of the position of the employee, systems is one of the biggest sources of operational risks. Particularly system-related problems which are visible to customers, because it causes reputational damage as well.

Information security failures are an operational risk which might create reputational damage along with financial losses. If sensitive customer information is accidently released to the general public, it could cause fines and other financial losses as well as reputational damage. Information security and failed data protection are both very often mentioned operational risks. The insurance business is very dependent on trust. Who would take insurance from an insurance company that cannot keep sensitive data safe. For this reason insurance companies take trustworthiness very seriously, another reason would be regulations.

Internal and external answers differ significantly in terms of regulations. In fact, internal interviewees did not mention any regulatory operational risks regarding Company X, whereas external interviewees raised multiple regulatory risks regarding their companies. The difference might be due to the position of the employees, however it is not the only explanation. The timing of the interviews is crucial, although interviewees received the questionnaire in advance. System-related operational risks were topical in Company X in the summer of 2014, clearly reflected in the answers, but this does not explain the difference either. It could be because only operational risk managers deal with regulatory operational risks or because Company X does not deal with regulations on a local level as much as other insurance companies in Finland. This might be due to fact that Company X has centralized operational risk management in one or two offices. In this case, "centralized" mean that offices around Europe do not have their own operational risks manager. This has been a business decision in where regulatory know-how might remain at the local level, excluding senior management, so regulatory risks are not part of daily processes in Company X. For example, the team that works with Solvency 2 is centralized in London. Regulations and regulatory supervision is a growing area, which is why it would be important to share information regularly on a local level as well.

However, if we look at the matrices in chapter 7 we can see that employees from other Finnish insurance companies talked a lot about regulatory operational risks. Money laundering, financing terrorism or statutory customers are already covered by regulations, and all of these create operational risks. Regulators demand that insurance companies do not participate in any criminal activity and that is why there are regulations that require better awareness of insurance companies' customers. Regulations that prevent criminal activity are very important, but they also create more costs for insurance companies. Again, if a company accidently takes part in, for example money laundering, it could be fined by the regulator. For MPIC there are statutory customers, meaning that Finnish law demands that MPIC's cannot choose their customers. Statutory customers are part of the regulations from Finnish authorities and might cause operational risks for Mutual Pension Insurance Companies. The influence of regulations on Finnish insurance companies could need further research.

Operational risks caused by humans have been noticed similarly in both matrices. Human error is the most common operational risk, which is hard to control completely. People can make a lot of different mistakes and every insurance company has to accept this. Of course, there must be controls, which expose mistakes before they cause

irreversible damage. Nevertheless, controls must be reasonable designed and carefully thought through so that they do not essentially complicate tasks. Setting controls is therefore balancing between reasonable and overbearing controls. Overbearing controls slow down operations so much that it is not wise to use them. A large number of controls might also be a motion of censure for employees, which clearly does not improve employees' motivation. Insurance companies should therefore go through the controls more regularly. Controls are a large part of the technological facilities which play a crucial role in people's work today. Technological development can make employees' tasks more difficult by changing all the time.

Employees in Finnish insurance companies think that technological development is an operational risk, but an opportunity as well. The biggest concern is that if a company does not keep up with technological development, it could cause major problems. The whole communication system is changing and companies have to be able to provide services in quickly updating channels. This means that if a company cannot keep up with development it has no future or, at least the future does not look very bright. Companies have to be able to provide services with different channels of distribution. If we do not provide these service channels someone else will and take our customers as well. Both internal and external interviewees were also concerned about hacking risks. Hackers have not been generally interested in insurance companies because there is not the same kind of money transferring as in banks, but when insurance companies centralize their sensitive data it could start to interest hackers. It is hard to say how criminals could use insurance companies' sensitive data in the future but insurance companies should pay attention to possible hacking problems brought about by technological development. Overall, the dependence is huge and it will not decrease, which is why insurance companies will have to spend substantial amounts of resources on the system in the future as well.

On the contrary, technological development removes certain kind of operational risks like typos and other human risks. More advanced technology might provide more support controls, reducing the number of mistakes. Growing automation will also help to minimize operational risks caused by human activity. Technological development also makes it easier to collect and edit data removing operational risks as well. The answers of the interviewees do not significantly differ here either. Everybody seems to agree that technological development is mandatory and companies should use the opportunities that it creates and be ready for the new operational risks that technological development entails.

Internal interviewees said that system-related operational risks were the most serious operational risks from the past. Again, Company X suffered minor system failures in the summer of 2014 therefore the system is raised when dealing with past operational risks. By contrast, external interviewees said that reputational damage had been the most serious past operational risk along with negative publicity. Insurance companies seem to be concerned about their reputation more than Company X. It could also be that because Company X is rather unfamiliar to Finland the media is not interested in Company X as much as in other Finnish insurance companies. MPIC in particular are under the scrutiny of the Finnish media and general public because of MPIC's role in the Finnish economy.

Systems were the main subject among the external interviewees regarding present operational risks as well, but external interviewees mentioned regulations as their present operational risks. Money laundering and financing terrorism are regulatory operational risks for today's insurance companies. Also changes in regulations can be segmented into operational risks. System failures on the other hand seem to be the main operational risks for Company X. There are significant differences in the past and present operational risks between Company X and other Finnish insurance companies, which could be due to differences in organizational structure. Research into the impact of organizational structure on operational risks in Finnish insurance companies is limited and could need further research.

System-related operational risks, such as securing sensitive information, will be a large part of operational risk management in Finnish insurance companies in the future due to the development of information technology. Insurance companies have to be able to react quickly to information technology development. In addition, regulations like legislative or political reforms could have a major impact on operational risk management in Finnish insurance companies in the future. All interviewees agreed on what could be operational risks affecting Finnish insurance companies in the future. Legislative and political reforms require companies to follow closely the development of the reforms. In addition, companies have to invest in relationships with regulators and other entities that might make changes to legislation. Cyber risks overall are a concern for Finnish insurance companies in the future. Cyber risks are dangerous because their severity or scope is still little known, making them unpredictable and difficult to prepare for.

How can Finnish insurance companies then prepare for operational risks? Monitoring and reporting realized operational risks are the most important part of the identification of operational risk that a company have. Every function defines their operational risks in a system. Operational risk management then maps the risks in a yearly report usually presented to senior management. Companies do not necessary have a particular system for operational risks, some uses excel and some have a modified risk management tool for operational risks. Company X uses the BWise risk management system for operational risk management as well as for other risks.

Likelihood	Consequences				
	Insignificant (<1tEUR)	Minor (1-10tEUR)	Moderate (10-100tEUR)	Major (100t-1mnEUR)	Catastrophic (>1mnEUR)
Very Likely (>30%)	High	High	Extreme	Extreme	Extreme
Likely (10-30%)	Moderate	High	High	Extreme	Extreme
Moderate (5-10%)	Low	Moderate	High	Extreme	Extreme
Unlikely (1-5%)	Low	Low	Moderate	High	Extreme
Rare (<1%)	Low	Low	Moderate	High	High

Figure 22. Likelihood and Consequences matrix

These reports that companies make are used to prioritize resources for operational risks. Companies have a person who is responsible for operational risks. This person usually raises a few important operational risks and prioritizing is done by the board of directors, with recommendations from risk managers. However, every function has powers of action, which means that they can make small decisions relating to small operational risk and usually only the biggest decisions go to the board of directors. Operational risk management is the only function which collects operational risks from other functions together in one report. Finnish insurance companies do not use calculations for operational risks as they use calculations for credit and market risk

because calculating operational risks is still rather difficult and special formulas for operational risks are rarely used. Insurance companies do not usually value Euros per risk in Finland. Some companies define operational risks with probability and effect using scales of one to five. This scale helps insurance companies to differentiate important operational risks from less important ones. This is a widely used tool to prioritize operational risks in Finnish insurance companies.

7.2 Answers to the Research Questions

This chapter answers the research questions. The key operational risks and most common tools used in Finnish insurance companies and Company X will be presented on the base of the answers of the interviewees. In addition, I will present how insurance companies in Finland prioritize their resources for operational risk management. Operational risk management differs slightly between Company X and other Finnish insurance companies as has been explained above. Despite these differences, they seem to manage operational risks quite similarly. Key operational risks in Company X and in other Finnish insurance companies can be put into four main categories. These categories are systems, human risks, technological development and regulations.

7.2.1 Key operational risks

System-related operational risks seem to be an issue for every insurance company in Finland, which is why companies might want to reallocate their resources. The function of the system is very important to an insurance company from the perspective of the management, employees and customers. It is hard to manage a company if the system does not work. In addition, employees get fatigued and tired if the system does not work and eventually some employees might leave the company. Of course if news of the system malfunction leaks to customers it causes reputational damage. This is why companies should take system malfunctions very seriously. Company X has taken steps to fix system weaknesses, which is good, but sometimes it would be better to look at the situation more holistically, not just repair minor errors.

Human risks are more low or moderate risks if we look at the likelihood/consequences table, but they occur more frequently and that is why companies should pay attention to them also. By reviewing controls and identifying the lack of controls they could reduce human mistakes. Internal fraud is very rare in Finnish insurance companies. Internal

fraud is currently prevented by controls so that potential opportunities for abuse are at a low level. Trust between employers and employees is at a good level, which is why no special controls are required. Actually Company X could review controls with a view to removing unnecessary and obstructive controls. Nevertheless, human risks are daily operational risks manageable with controls and good communication. Companies can always improve internal communication, for example by aligning different functions, which might reduce unnecessary communication. Better communication is an essential part of human risk management. In addition, technological development can help to reduce human risks.

Technological development can be mentioned as one of the key operational risks in Finnish insurance companies. Technological development and dependence is an opportunity and a threat to an insurance company. If a company does not keep up with technological development it cannot provide customers with proper digital services, this may incur customer losses. Keeping up with technological development is actually a mandatory requirement in the current, competitive, economic environment. An insurance company has to take technological development very seriously if it wants to succeed against the ever-increasing competition. Technological development exposes a firm to more fatal system failures therefore management has to pay serious attention to it. Technological development can also expose insurance companies to new cyber risks such as hacking or sensitive customer data abuse. Securing sensitive data is very important and developing information technology can make the information environment more vulnerable.

The fourth key operational risk would be regulations. Continually strengthening the role of the regulators creates more work for insurance companies. Insurance companies have to follow regulators so that new regulations do not come as surprises. Regulations like legislative reforms might cause changes to processes, which is why it is important to know about regulatory changes in advance. Already existing regulations, like financing terrorism and money laundering, cause additional work for insurance companies. If companies do not comply with regulations it may result in substantial fines. Regulations do not exist simply to annoy companies, a high-level regulatory framework makes it easier, providing continuity and knowledge as well. All of the four key operational risks which occur in Finnish insurance companies would benefit from more specific research.

7.2.2 Most common tools

Finnish insurance companies all use rather difference tools for operational risk management. This is because operational risk management has not yet found the most functional model. Operational risk management is still quite young, which is why different tools or models are still competing with each other. However there are some similarities between the tools that insurance companies use in Finland. here is a clear tendency is to give probability and consequences rates to operational risks. This is how companies specify operational risks, providing better knowledge when prioritizing operational risks. The likelihood and consequences table introduced earlier in this study is a simple version of a tool that has been used in operational risk management.

Nevertheless, tools that Finnish insurance companies use remain fairly simple. Some use excel to record operational risks, some have more advanced tools, Company X for example uses the BWise system for operational risks recording. Currently, insurance companies monitor, make reports and try to control operational risks that have been found. In addition, Finnish insurance companies do not actually use any relevant tools to calculate operational risks. Insurance companies do not measure operational risks as they measure credit and market risks. This might be one subdivision which might need more attention from risk management in Finnish insurance companies. The simple level of operational risk management tools is perhaps due to the fact that operational risks are a relatively new risk category in the insurance business in Finland. By contrast, banks use much more advanced operational risks management tools. Could these tools be used for the insurance business as well?

7.2.3 How to prioritize resources to operational risks

How do insurance companies then prioritize resources for operational risks using the tools that they have? The first action that companies take is to look at the watch list of operational risks. Risk management then rates the operational risks that appear on the list using, for example, the probability x consequences method. This is how operational risk management knows which operational risks are the most important and which ones are less important. After rating them, operational risk management analyse what kind of actions certain operational risks need and should they report to senior management or can they execute actions by themselves. Minor operational risks can be usually be remedied by the business section that is under the influence of the operational risk. On

the other hand, if the detected operational risk is larger and needs structural changes to fix, the operational risk manager informs senior management. Senior management then make the decision. It usually happens once or twice per year that the operational risks manager informs senior management about operational risks. However, if the risk is severe and company should immediately react, then senior management usually participates quicker.

Insurance companies in Finland do not have many different ways or methods for prioritizing operational risks. The simple way that they use is to give values to operational risks for its likelihood and impact. The evaluation of likelihood and impact is based on feelings and experience. This is not a sufficient way to evaluate the likelihood and impact of operational risks. However, there are no formulas or methods which would be unambiguously better for prioritizing operational risks, with the exception of the AMA model used by the world's largest banks.

8. CONCLUSIONS

This research opens up new research directions for operational risk management within what companies can explore in order to improve performance. This study shows that there are four main operational risks that concern insurance companies in Finland. These operational risks are systems, human risks, technological development and regulations. System-related operational risks especially seem to cause problems for insurance companies in Finland. Companies know that system-related operational risks create costs but have no further details. Thus, companies such as Company X should pay more attention to details that create system-related operational risks. In order to do so, they should improve communication channels between IT and operations, examine controls in order to improve response speed and arrange the processes to support the system more systematically. System-related operational risks are distinctly internal operational risks unlike technological development, but these two are essentially connected to each other. Technological development is inevitable for insurance companies that want to stay in the globally competitive. Customers demand faster and easier channels to communicate with companies. Sending letters is old hat. However, investing in technological development is very expensive and long term. Sometimes it is still a better choice to acquire a new system than repair the old one. These are decisions that senior management should bring up regularly. Although technological development can be a business risk it also creates numerous operational risks as well, which means that operational risk management should take part in decisions concerning technological development.

In addition, human risks and regulatory risks are key operational risks for insurance companies in Finland and for Company X. Even though they are not as topical as system-related operational risks or technological development they are still a very important part of operational risk management. In fact, regulatory risks will increase in the future therefore insurance companies should prepare for them as well as they can. It could facilitate the operative sector in the future when new regulatory demand may appear. Regulatory violations have caused major damage to banking sector, this should serve as a warning to insurance companies. It has been said that solvency 2 will update regulations for insurance companies in the near future. This study shows that insurance companies could prepare better for regulatory operational risks. How they could prepare better should be researched in another study. However, Company X could concentrate more specifically on a local level when dealing with regulatory operational risks.

Operational risks caused by people can be found in all insurance companies in Finland. In particular, communication and dependence on an individual employee are the most important operational risks that people incur. Company X should focus on and improve communication channels so that there would be no damaging misunderstandings. They should also hold on to key employees to make the continuous of the company more secure.

Quantitative calculations for operational risks are still quite rare in Finnish insurance companies, which indicate that insurance companies are in the early stage of development when dealing with operational risks. Insurance companies could try to take inspiration from the banking sector, which uses more advanced quantitative methods for operational risks such as AMA. However, the most common tool that Finnish insurance companies use is a likelihood and consequences matrix. This matrix is quite simple yet functional. The matrix tells a company which operational risks are worth the effort and which are not. By improving this tool, insurance companies could obtain more useful information about operational risks and then be more prepared. Nevertheless, it could need more specific research in order to make it more useful.

Finnish insurance companies prioritize their limited resources for operational risks by giving values to different operational risks. By giving these values, operational risk management map the importance of the operational risks and then prioritize resources for the most important. Values can be given with a likelihood and consequences matrix or with some other similar method. However methods that are used are quite simple therefore the allocation of the resources does not always go perfectly. These methods need more study so that insurance companies could be more precise when allocating resources. For now, the values are based on historical knowledge or even a belief. It should be more quantitative and specific.

At the end it is important to assert that operational risk management is a vital part of the companies' short and long-term success. Insurance companies in Finland should take operational risk more seriously in order to avoid any unpleasant surprises. However this study just scratches the surface of operational risk management; further research would certainly help to develop a framework for managing these risks in the insurance industry.

REFERENCES

Abrantes-Metz Rosa M., Michael Kraten, Albert D. Metz & Gim S. Seow (2012). Libor manipulation? *Journal of Banking & Finance, 36:1, 136-150.*

Buchelt, R. and S. Unteregger. (2004). Cultural Risk and Risk Culture: Operational Risk after Basel II. *Financial Stability Report 6*

Cacouette, John B. & Altman, Edward I. & Narayanan, Paul (1998). MANAGING CREDIT RISK: The Next Great Financial Challenge. John Wiley & Sons, Inc. Canada (1998).

Cambell Alexander (2012). Top 10 operational risks for 2013. *Operational Risk & Regulation, Operational Risk, 2012.*

Carter, R. L. & Doherty N.A. (1975). Handbook of Risk Management. Kluwer-Harrap Handbooks, Rembrandt House, 529 London Road, Isleworth.

Carol Alexander (2000). Bayesian Methods for Measuring Operational Risk. *Discussion papers in finance 2000-02.* University of Reading, UK. P. 2-22.

Cassel Catherine & Gillian Symon (2004). Essential Guide to Qualitative Methods in Organizational Research. SAGE Publications Ltd, London 2004.

Chavez-Demoulin V, P. Ebrechts & J. Nešlehová (2006). Quantitative models for operational risk: extremes, dependence and aggregation. *Journal of Banking & Finance, 2006, 30:10, 2635-2658.*

Clarke Chiristopher J. & Varma Suvir (1999) Strategic risk management: the new competitive edge. *Long Range Planning, 1999, 32:4, 414-424.*

Cruz, M. G. (2002). Modelling, Measuring and Hedging Operational risk, John Wiley & Sons Ltd. West Sussex, UK.

Danielsson, J., H. S. Shin and J. P. Zigrand (2004). The Impact of Risk Regulation on Price Dynamics. *Journal of Banking & Finance, 28:5, 1069-1087.*

Denzin Norman K. & Lincoln Yvonna S. (2011) The SAGE Handbook of Qualitative Research. SAGE Publications, Thousand Oaks, California, 2011.

Directive 2009/138/EC of the European Parliament and of the Council (2009). *Taking up and Pursuit of the Business of Insurance and Reinsurance (Solvency 2).*

Duffie Darrel & Singleton Kenneth J. (2003). Credit Risk: Pricing, Measurement and Management. Princeton University Press, 41 William Street, Princeton, New Jersey (2003)

Esterhuysen Ja'nel, Gary van Vuuren & Paul Styger (2010). The Effect of Stressed Economic Condition on Operational Risk Loss Distributions. *Sout African Journal of Economic and Management Sciences, 13:4.* University of Pretoria, On-line version ISSN 2222-3436.

Gregoriou Greg N. & Lhabitant Francois-Serge (2009). Madoff: A Riot of Red Flags. *Edhec Risk and Asset Management Research Center, Lille-Nice, 2009.*

Hadjiemmanuil Christos 2003. Legal Risk and Fraud: Capital Charges, Control and Insurance. *Operational Risk: Regulation, Analysis and Management, Hall-Financial Times.*

Herring J. Richard (2002). The Basel 2 Approach To Bank Operational Risk: Regulation On The Wrong Track. The Wharton School University of Pennsylvania, 2002.

Hoffman Douglas G. (2002). Managing Operational Risk: 20 Firmwide Best Practice Strategies. Published by John Wiley & Sons, Inc., USA, New York.

Imad A. Moosa (2007). Operational Risk: A Survey. *Financial Markets, Institutions & Instruments, 16:4, 167-200.*

Jarrow A. Robert & Turnbull M. Stuart (2000). The Intersection of market and credit risk. *Journal of Banking & Finance, 2000, 24:1-2, 271-299.*

Jickling Mark (2002). The Enron Collapse: An Overview of Financial Issues. *CRS Report for Congress, Government and Finance Division, 2002. http://fpc.state.gov/documents/organization/8038.pdf*

Jobst Andreas A. (2007). The Sting is Still in the Tail But the Poison Depends on the Dose. *Journal of Operational Risk, 2:2, 435-449.*

Järvinen Raija, Lehtinen Uolevi and Vuorinen Ismo, (1998). Content and measurement of productivity in the service sector. *International Journal of Services Industry Management, 9:4, 377-396.*

Kaufman George G. and Kenneth E. Scott (2000). Does Bank Regulation Retard or Contribute to Systemic Risk. *Standford Law School, John M. Olin Program in Law and Economics, Working Paper 211.*

Pezier Jacques (2002). Operational Risk Management. *ISMA Discussion in Finance 2002*. University of Reading, UK. P. 4-5, 23-24.

Loader, David (2007). Operations Risk: Managing a Key Component of Operational Risk. *Butterworth-Heinemann 2007, 189.* Jordan Hill, GBR.

Lopez, Jose A. & Saidenberg, Marc R. (2000). Evaluation Credit Risk Models. *Journal of Banking & Finance,* 24:1-2, 151-165.

Lopez, Jose A. (2002). What is Operational Risk? *FRBSF Economic Letter, 2002-02; January 25, 2002.* Economic Research And Data.

Madill Anna, Jordan Abbie & Shirley Caroline (2000). Objectivity and reliability in qualitative analysis: Realist, contextualist and radical constructionist epistemologies. *British Journal of Psychology, 91, 1-20, 2000)*

Marshall, Catherine & Rossman Gretchen B. (1998). Designing Qualitative Research 3rd edition. SAGE Publications, 1999.

Raghavan R. S. (2003). Risk Management In Banks. *Chartered Accountant, New Delhi, February 2003, 841-851*

RandMark40. Insurance Data Platforms. *Abrief history of insurance.* http://www.randmark40.com/index.php?option=com_content&view=article&id=33&Itemid=56

Roberts Alexander, William Wallace & Neil McClure (2003). *Strategic Risk Management.* Edinburgh Business School, Heriot-Watt University, Edinburgh, United Kingdom, 2003.

Schlesinger Harris (2013). The theory of Insurance Demand. *Handbook of Insurance, 2013, pp. 167-184.*

Sosiaali- ja Terveysministeriö (2015). Vakuutusasiat. http://stm.fi/vakuutusasiat

Taloussanomat (2008). Sampo Pankin Kriisi. *Taloussanomat, juttusarjat, Sampo-pankin-kriisi, 2008. http://www.taloussanomat.fi/juttusarjat/sampo-pankin-kriisi.*

The Statistical Portal (2014) The Largest Insurance Companies Worldwide in 2014. *http://www.statista.com/statistics/270998/worlds-largest-insurance-companies-by-total-assets/*

Tilastokeskus (2013). Vakuutustoiminta 2013. *Rahoitus ja vakuutus 2014. http://tilastokeskus.fi/til/vato/2013/vato_2013_2014-11-12_fi.pdf*

Turing D. (2003). Advances in Operational Risk: Firm-wide Issues for Financial Institutions 2003, p: 253-266.

Vinella P. and Jin J. (2005). A Foundation for KPI and KRI. *Operational Risk & Regulation, Operational Risk, Practical Approaches to Implementation p: 157-168, 2004.*

Walker Peter (2012). UBS rogue trader Kweku Adoboli jailed over 'UK's biggest fraud. *The Guardian, Tuesday 20 November*.

APPENDIX

Operative risks: General questionnaire

1. Is the term operational risk familiar? (yes/no)
2. Would you mention few realized operational risk that has occurred in Finland or worldwide?
3. What kind of daily operational risks your company face?
4. What kind of tools your company use in:
    a) Identification of operational risks,
    b) Calculation of operational risks,
    c) Prioritize of operational risks?
5. How much resources you have available for operational risk management? (Employees, money, time)
6. Do the regulations of operational risks (e.g. Solvency 2, Basel 3) have an affect to your business? How?
7. Would you mention the order of five or more biggest/most important operational risk regarding your company in the following categories?
    a) Already realized operational risks
    b) Now faced operational risks
    c) Possible operational risks emerging in future
8. Are the processes of your company part of the operational risk management?
9. How great risk/threat is the development of the technology and its constantly growing dependence to your company?
10. Is the lack of controls caused operational risks to your company?
11. What is in your opinion the single largest realized operational risk? And how do you think it could have been prevented? (You can also mention the more than one).
12. Would you mention some operational risks, which can be devastating in the future?

Operatiiviset riskit: Sisäinen kyselylomake

1. Onko teille tuttu termi operatiivinen riski?(kyllä/ei)
2. Mainitse muutama maailmalla tai Suomessa toteutunut operatiivinen riski.
3. Minkälaisia päivittäisiä operatiivisia riskejä teidän mielestänne yrityksemme kohtaa?
4. Kuinka suurena riskinä näet teknologian kehityksen ja sen aiheuttaman yhä suuremman riippuvuuden yrityksellemme?
5. Minkälaisia työkaluja meillä on käytössä:
    a) operatiivisten riskien kartoittamisessa,
    b) operatiivisten riskien laskennassa,
    c) operatiivisten riskien priorisoinnissa?
6. Miten nämä työkalut eroaa aiemmista työpaikoistanne?
7. Mainitse järjestyksessä neljä(tai enemmän) tärkeintä/suurinta operatiivista riskiä koskien yritystä X seuraavista kategorioista:
    a) jo toteutuneita operatiivisia riskejä
    b) tällä hetkellä tuoreita/pinnalla olevia operatiivisia riskejä
    c) mahdollisesti tulevaisuudessa ilmeneviä operatiivisia riskejä
8. Miten mielestäsi toteutuneisiin ja pinnalla oleviin riskeihin olisi voitu valmistautua paremmin? Miten ne olisi voitu välttää?
9. Kuinka suurena operatiivisena riskinä näet väärinmyydyistä tuotteista aiheutuneet kustannukset? Millä toimenpiteillä pienentäisit niistä aiheutuvia riskejä/kuluja?
10. Miten operatiiviset riskit eroavat yrityksestä X ja yrityksessä/yrityksissä missä työskentelitte ennen?
11. Osaisitko mainita joitain tulevia operatiivisia riskejä, joihin ei välttämättä osata vielä varautua?

* Tuleeko teille vielä mieleen muuta mainitsemisen arvoista?