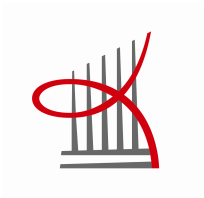

INFORMATION AND KNOWLEDGE RISK MANAGEMENT AT COMPANY X

Silja Niemistö

Bachelor's thesis
November 2013
Degree Programme in International Business

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in International Business
NIEMISTÖ, SILJA
Information and Knowledge Risk Management at Company X
Bachelor's thesis, 74 pages
November 2013

This study was made for company X, a company operating in corporate gift business. Risk management was chosen to be the field of study since there wasn't any actual risk management process started in the company. However, due to the extension of entire risk scope it was decided that the study would cover only one risk category. Since the firm's success was largely reliant on effective use of information and knowledge, risks related to this area were assumed to require urgent management and thus chosen to be the object of research. The goal of the study was to initiate information and knowledge risk management at company X by analysing its current risk profile and suggesting how the company could manage its current and future risks. Ethnography and qualitative interviews were used as research methods

For information security reasons detailed findings and recommendations were left out from this public report and replaced by blank pages. The study revealed that company X had as much as seven substantial information and knowledge risks. Since simultaneous actualisation of two or more of these risks could have been fatal, it was recommended for the company to start taking action right away. Fortunately, the analysis unveiled that several information risks could be diminished by rather simple and inexpensive means. The management of knowledge risks appeared to require high involvement from company X's management. However, when thoroughly implemented, knowledge management process would not only reduce risks but build competitive advantage as well.

This study succeeded to provide a good starting point information and knowledge risk management at company X. Since some of the results were quite unexpected they were also apt to awake the interest of company managers. Nevertheless, the actual implementation of suggested measures was left for the organisation to decide about.

Keywords: information, knowledge, risk management

TABLE OF CONTENTS

1 INTRODUCTION

The significance of information in business is constantly increasing due to extensive possibilities of storing and sharing data with fast developing information technology. The change has been so quick that many businesses haven't still realised how prominent assets information and knowledge actually are for them. Neither have they realised how substantive threats there are related to this area. As the operations of most businesses, especially in the western world, are nowadays mainly based on information processing it has become crucial for them to manage their information and knowledge. (Liiketoimintaa Turvallisesti 2012, 22-23.)

This study is conducted for company X, a family enterprise operating in the field of corporate gifts and promotional products since 1998. Company X mostly retails to other businesses, but wholesaling comprises a part of the sales as well. Company X also imports part of the products. In the beginning the firm's main focus was on giveaway products, but the product range has gradually expanded and currently covers also exclusive gift products, special promotional material and a variety of textiles. Company X has 13 employees four of whom work in the branch office in Espoo and the rest in Tampere where the head office is located.

Company X doesn't manufacture anything itself, but all the products are supplied from a massive number of other businesses. Due to this fact company X's staff has to either possess the knowledge or find the information for using suitable suppliers for each product. In order to maintain good product quality and competitive prices it is crucial that the right suppliers are used and the production process controlled as carefully as possible. Since company X's sales are based on good long-term customer relationships it is especially important that knowledge of serving each customer to the full is preserved. Another prominent factor in building customer relationships is that information concerning customer history gets recorded.

The aim of this thesis is to initiate information and knowledge risk management at company X. The process will be put into practice by analysing the current risk profile and suggesting an action plan for managing information and knowledge risks now and in the future. The subject was proposed to company X's CEO, after the author had completed her practical training period at the firm. Analysis of Company X's opera-

tions revealed that the company's success was mainly built on the information and knowledge it possessed. Company X had also taken a great step towards “paperless office”, which had enhanced the need for electric data protection. However, there hadn't yet been much action taken for managing information and knowledge. The author decided to approach the subject from the angle of risk management, since increased awareness of risks was assumed to function as a motivator for company X's management.

There are no earlier studies conducted for company X concerning information and knowledge issues. Neither have any kind of risk analyses been executed before. The lack of existing data increases challenges related to this study since the author can only use similar studies conducted for other organisations as back-up material. However, general data concerning risk management is well available. “PK-yrityksen riskienhallinta (PK-RH)” website, especially designed to correspond the risk management needs of Finnish SME:s, is one of the main sources of information used for this thesis. Other principal information sources are risk management material written by Arto Suominen (2003), Hannu Kuusela and Reijo Ollikainen (2005), information security guidelines provided by Confederation of Finnish Industries (EK) and Kate Andrew's extensive work among knowledge risk management.

Table 1 illustrates the scope of this thesis. The main areas of company X's risk field are presented on the top and the four steps of risk management process are listed one below another on the left side. The blue cells illustrate the risk management area this study focuses on whereas the grey cells represent the risk categories and management actions still remaining unstudied. (PK-RH 2013.)

TABLE 1. Thesis scope

Risk Field / **Management process**	Business risks	Environ-mental risks	Information and knowled-ge risks	Product risks	Personnel risks	Agreement and liability risks
1. Identification and assessment						
2. Definition of suit-able risk management methods						
3. Preparing for loss						
4. Review and learn-ing from incidents						

This thesis starts from theoretical study which will mainly focus on risk management process and the special characteristics of information and knowledge risks. After theoretical framework chapter three will present the research methods and the planned execution process. Research findings will be reported in detail in chapter four. Subsequently, chapter five comprises of the recommendations aimed for company X's management. Finally, chapter six will conclude the entire study.

What makes this paper unique is that there are no risk analyses conducted for company X before, thus this study acts as forerunner for new studies and risk management actions to come. Another factor setting this paper apart from previous research is that it combines information and knowledge risk management. The author didn't find any former study merging these two concepts which, after all, are very closely linked to each other.

The fact that no previous risk management material exists in company X causes a limitation for this study since there is no baseline for reference. Another limitation is the author being employed by company X during the research process, which may have a slight effect on objectivity of the findings.

2 THEORETICAL FRAMEWORK

This chapter will discuss the theory behind this research. Risk nature and characteristics will be presented at first. After that the text will continue to introducing overall risk management theory to the reader. Once the general risk management process has been discussed the chapter will continue to deal with information security. Subsequently, the text will proceed to information risk management. Finally the relatively new concept of knowledge management will be presented.

2.1 Risk characteristics

In spoken language the term risk is used when there is a possibility that something unpleasant may happen. There are different definitions for the term depending on the perspective. Risk may be seen as a condition where the final result differs from desired outcome. The term “risk” is usually understood as danger or possibility for an accident. However, risks can also be perceived as freedom and courage to choose in which direction to head. As a matter of fact, a slow change can be noticed in risk perception today. Even though people still see IT-development, competition etc. as risks we are starting to see these factors, not merely as threats, but as opportunities as well. (Kuusela & Ollikainen 2005, 16-17, 35.)

Risks can be classified according to their consequences and the field they concern. Categorisation after consequences is used especially when insurance cover is applied since some risks are uninsurable depending on the consequences. If the risk can lead to either profit or loss it is called dynamic or speculative risk. Business risks belong to this category since they always aim at profit, but the possibility of loss is around as well. Usually the appearance and size of these risks can be controlled by the risk taker thus these risks are uninsurable.(Kuusela & Ollikainen 2005, 33-34.)

Static risks, also called pure risks, can only lead to loss or no loss hence they never bring any benefit. Examples of these risks are, for instance, death of an employee or destruction of property. Pure risks can be insured since they can be forecast better than speculative risks. Fundamental risks have an effect on a large group of people. Examples of these risks could be war of inflation. There are also particular risks such as

theft, accident or disease which affect only one individual. These risks are usually insurable, but the particular individual accounts to the insurance cover by him-/herself. (Kuusela & Ollikainen 2005, 33-34.)

In order to facilitate assessment risks are often classified according to the area they concern. Common risk types in business are personnel risks, contract and liability risks, information risks, product risks, environmental risks, project risks, interruption risks, crime risks, fire risks and business risks which are crucial in strategic sense. (PK-RH 2013.)

2.2 Risk Management

Entrepreneurship and risks go hand in hand. That is to say, entrepreneurship cannot exist without risks since the implementation of new ideas and innovations can always have unexpected consequences. However, risks can be anticipated to some extent which enables companies to minimise the expenses. Companies that have implemented an effective risk management programme are able to take controlled business risks and by that means secure their success. (Kuusela & Ollikainen 2005, 66-67; Suominen 2003, 51.)

Risk management used to be seen as a separate, narrow area of management. Later on, that kind of approach appeared ineffective thus today the aim is to integrate risk management to business strategy. Risk management should be seen as a permanent tool which is used whenever planning the future. It is also important to see risk management as a common goal of everybody. Thus, not only one person should be responsible of managing risks, but everyone's actions count. Still in many firms risk management is seen more as a project than process. Only by changing this view companies can clearly benefit from the choices they make. SME:s often find optional insurances too expensive hence focus on strategical decisions and establishment of secure standards of activity may be essential for these companies in order to secure their business.(Kuusela & Ollikainen 2005, 155-157, 166; Suominen 2003, 27-30.)

The core idea in risk management is that the company should be able to continue in business, no matter what risks came true. Thus businesses should be able to bear the

costs originating from risks that come true. This necessitates analysis of potential risks and their consequences. Careful definition of the company's risk profile acts as a cornerstone for Risk management. Even though the process takes time and effort, especially in the beginning, the benefits of thorough implementation will exceed the costs deriving from execution. (Kuusela & Ollikainen 2005, 155-157.)

It is important that the implemented risk management program is proportioned to the size of the company. There are many risk management tools and standards available for companies to utilise, but they tend to be too heavy tools for SME's use. However, regardless of their size it is equally important for all companies to integrate risk management to their overall business strategy. Suitable risk management tools and materials for SME:s is provided by PK-RH (Risk Management for Finnish SME:s) website which is particularly designed for the use of Finnish SME:s. The website contains risk management tools, such as check-lists and useful information about risk identification and assessment. Insurance companies are another party providing suitable tools for SME:s. (Kuusela & Ollikainen 2005, 156-157; PK-RH 2013; Ovatko yrityksesi tietoriskit hallinnassa? 2001, 16-17.)

2.3.1 The four-phase model of risk management

PK-RH website presents the risk management process in a four-phase model (figure 1):
1) Risk identification and assessment
2) Risk management methods
3) Accident anticipation
4) Follow-up and learning from accidents

FIGURE 1. The four-phase model of risk management (PK-RH 2013)

In the first phase risks are identified and assessed by going through each risk type at a time. The most accurate results are achieved when the process is executed in cooperation. Since risk identification requires good imagination and experience of different kinds of jobs in the firm it is important to get the staff involved. Check-lists or other tools can be used to facilitate risk identification. One example of a check-list available in PK-RH website is presented below (figure 2). This kind of check-lists are useful, but it has to be kept in mind that they are only directional. Namely, each company has a different variety of risks to consider and many of those risks are not mentioned in check-lists. (PK-RH 2013.)

FIGURE 2. Business risk check-list (PK-RH 2013)

Once all the risks occurring to the participants have been noted their consequences are to be assessed step by step. The consequences may be of various kind: for example, strategic, financial, interruptive, reputation or health consequences. Mathematically risks are considered as likelihood and they can be assessed by the following formula:

risk = likelihood x severity (Suominen 2003, 10, 12-19.)

Consequences of certain risks are difficult to assess in financial terms. For example, it's hard to say how large expenses reputation risks would cause when coming true. It is also difficult to estimate the exact likelihood of risks coming true especially if there

are no records of actualized risks. Because of this risk probability and severity are usually assessed in a rough three- or four-step scale. PK-RH website divides risk probability in three categories: highly unlikely, unlikely and likely. Consequences are categorised accordingly as slightly harmful, harmful or extremely harmful. Risk assessment in three-step scale is demonstrated in table 2 below. (Reputation Risk Takes Center Stage 2009; PK-RH 2013.)

The likelihood of the harm	The severity of the harm		
	Slightly harmful	Harmful	Extremely harmful
Highly unlikely	1. Trivial risk	2. Tolerable risk	3. Moderate risk
Unlikely	2. Tolerable risk	3. Moderate risk	4. Substantial risk
Likely	3. Moderate risk	4. Substantial risk	5. Intolerable risk

TABLE 2. Three-step risk assessment scale (PK-RH 2013)

The assessment scale can be divided in as many categories as needed depending on how accurate results are aimed at. The categorisation should always be planned according to the company in question since, for instance, loss of one million € may be medium loss for one and catastrophic for another company. Categorisation of risk severity is usually based on losses resulting from risks coming true whereas risk probability assessment is founded on frequency. For instance, slightly harmful consequences could correspond losses of less than 10 000€, harmful consequences less than 100 000€ and extremely harmful losses of more than 100 000€. When it comes to probability highly unlikely risks could, for instance, be defined as those taking place once in a hundred years, unlikely risks once in a ten years and likely risks once in a year. (Suominen 2003, 20-21; PK-RH, 2013.)

In order to point out the most dangerous risks each likelihood and severity category is given a multiplier. In the case of three-step categorisation the multiplier is 1 for slightly harmful and highly unlikely risks, 2 for harmful and unlikely risks and 3 for extremely harmful and likely risks. Thus a risk which is harmful (multiplier 2) but highly unlikely (multiplier 1) totals a value of 2 whereas a slightly harmful (multiplier 1) but likely risk (multiplier 3) totals a value of 3. Once all the risks are assessed by this means it is easy to point out the most significant risks which total the largest values. (PK-RH 2013.)

Once consequences of different risks are assessed it is time to consider what kind of action should be taken in order to manage them. The primary methods are avoiding the risks or diminishing the harm resulting from them. The most severe risks should be mitigated at first since their actualisation cost may be too much to handle. However, when it comes to smaller risks, sometimes the most suitable means of control is preparation for consequences. It is important to note that all the risks cannot be eliminated and even if they could it would make no sense. As a matter of fact, too little control leads to big losses deriving from risk actualisation whereas too much control leads to control actions being more costly than the risk themselves. (PK-RH 2013.)

Risk expenses are illustrated in figure 3 below. Total risk expenses curve is formed by adding retention costs to transfer costs. Total expenses reach their optimum (minimum) point when risk retention and transfer cost curves intersect each other. Suominen (2003, 116-117) has added also risk control costs to the transfer costs which would make the curve even steeper. (Suominen 2003, 116-117; Fundación Mapfre 2010.)

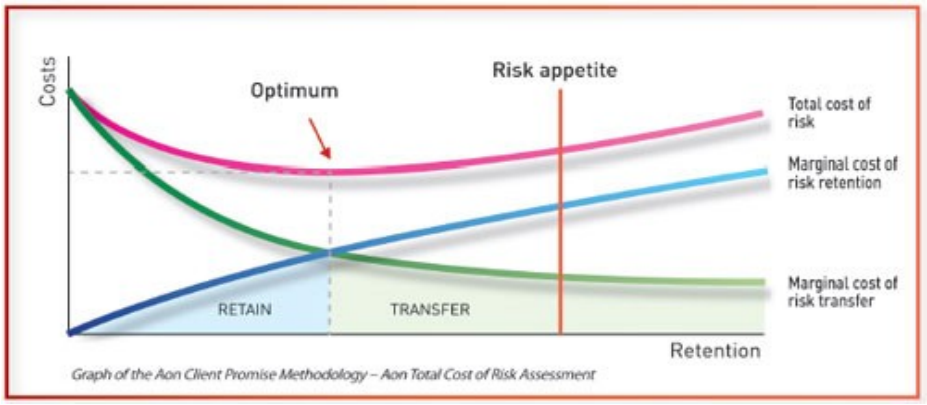

FIGURE 3. Total risk expences (Fundación Mapfre 2010)

Suominen (2003, 143) states that in order to reach a balance between risk control and retention the risks which cause minor losses but occur often should be kept. Also bigger risks can be kept if they are less probable and if their consequences are either small or medium. However, when it comes to risks with significant consequences none of them should be kept. According to PK-RH website (2013) risks with catastrophic consequences should be eliminated and those with significant consequences reduced immediately. When catastrophic or significant risks are in question the high-risk operations should be interrupted until preventive action has been taken. Actions concerning moderate risks should be carefully thought in order to avoid excessive costs. Small

risks should be kept unless their control is costless and easy. (PK-RH 2013; Suominen 2003, 143.)

There are four methods for dealing with risks: avoidance, reduction, transfer and retention. These risks management methods can be divided in two categories: risk control and risk financing. This categorisation is illustrated in figure 4. When it comes to risk control the focus is on the causes while risk financing is related to effects. Risk avoidance and reduction are ways for controlling the risks whereas risk transfer and retention result in risk financing. (PK-RH 2013; Suominen 2003, 98-100.)

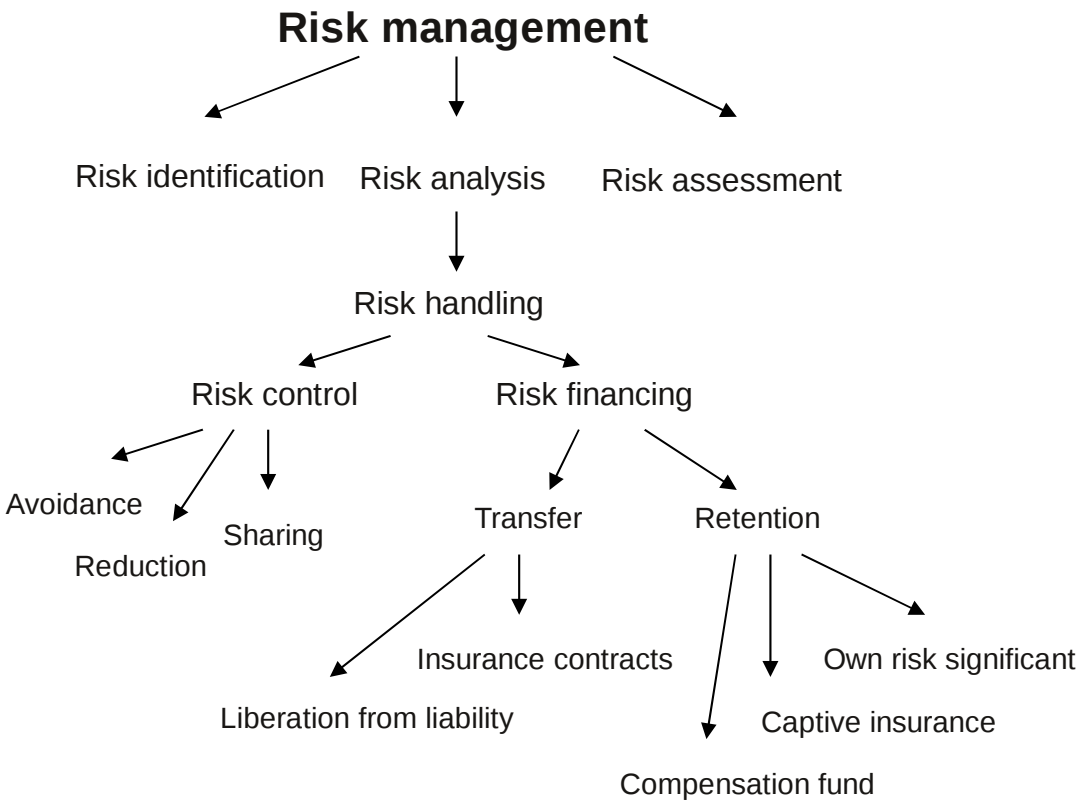

FIGURE 4. Risk categorisation (Suominen 2003, 99)

Ways of avoiding risks are, for example, refusing from taking a business risk or acquisition of a generator which keeps the operations going during power failures. When it comes to risk reduction the aim is to reduce the probability of a risk or seriousness of its consequences. One way of risk reduction is risk sharing which means that the risk object is shared into smaller sections. For example, by dividing the functions of a company in offices located on different districts it is possible to reduce the harm caused by

fire, burglary etc. Arranging first-aid training for staff is also one example of risk reduction. (PK-RH 2013; Suominen 2003, 100-105.)

When insurances are taken risks get transferred and the insurance company becomes liable for the financial consequences of those risks. Risks can also be transferred by supplying some risky function from another company. Anyhow, there are also cases where risk retention is the best option since preventive actions are sometimes more costly than risk keeping. For example, some convenience stores suffer from constant shoplifting due to small number of staff. However, this risk is kept since it would be more costly to hire more employees. (Suominen 2003, 114-117; PK-RH 2013.)

The third phase of risk management process, accident anticipation, aims at planning effective ways for clearing the situation after risk actualisation. All the significant risks should be reviewed in beforehand and a procedures established for the cases of accident. Accidents can be anticipated, for example, by instructing organisation members on action to be taken whenever a certain risks actualises. (PK-RH 2013; Suominen 2003, 100.)

After accidents have realised they shouldn't be forgotten. Thus the fourth phase of risk management includes learning from accidents. Accidents are a good source of learning thus they should be analysed carefully and with the focus on potential preventive actions. The bigger the accident the more attention it should be paid on. It is also worth noticing that accidents that were close should be considered as well. (PK-RH 2013.)

In follow-up the actualised risks are analysed as a whole. Risk follow-up meetings should be arranged regularly, for instance, once a year and the agenda should include review of the previous year, analysis of the current situation and risk plan update. Usually, some risks have disappeared and some new threats emerged. Since the situation changes all the time it is important to keep on track with those changes. (PK-RH 2013.)

2.3.2 Insurance –traditional risk management method

Insuring is the traditional means for risk management. In the past it was seen as the most important way of controlling threats. Companies have certain compulsory insurances such as pension insurance. However, the compulsory insurances provide protection only for a small fraction of the risks. Nevertheless, when the total number of insurances taken by companies is concerned voluntary insurances make up only less than 20% whereas the rest are compulsory. This phenomenon may partly derive from companies not realising the importance of risk management and insurance taking. On the other hand the reason for this kind of division may be the change in risk management methods. Namely, more and more companies are starting to manage their risks by taking control over them. (Kuusela & Ollikainen 2005, 155; Suominen 2003, 126-127.)

When information and knowledge risk management is concerned companies seldom rely on taking insurance. This phenomenon derives from the abstract nature of information which hampers definition of the insured object. It is also true that certain consequences of information risks, such as deterioration of company reputation, cannot be thoroughly compensated by money. In addition, information and knowledge risks are usually more effectively managed by other means. (Suominen 2003, 81-84.)

There are different types of insurance solutions available for companies, and the most typically chosen insurance covers the costs of fires, electricity problems, property crimes and leak damage. If necessary, the protection can be extended further, even to all-risk level. Even though insuring information is problematic there are some solutions available for that as well. For example, property insurance can cover, hardware, printers, servers, accessory equipment etc. (Suominen 2003, 126-133.)

Another insurance used for covering the costs of information risks is business interruption insurance which bears the costs resulting from interruptions in the business. This insurance can cover property interruptions, dependence interruptions or accident interruptions. Accident interruption means that key person becomes unable to work whereas property interruption stands for material damage interrupting the business. Dependence interruption takes place, for example, when a crucial supplier faces business interruption which in turn leads to interruption in their client's business. Interruption insurance can be used for refunding the sales margins lost during the interruption or for

refunding the costs deriving from clearing the situation, overtime work and special arrangements. However, the costs will be covered only if the company complies with the contract terms and takes agreed action to secure the insured objects. (Yritysturva Omaisuus-, keskeytys-, vastuu- ja oikeusturvavakuutukset 2012, 16-18; Suominen 2003, 132-133.)

When information risks are concerned accident and property interruption insurances can be used for transferring some indirect costs to the insurance company. However, insurances aren't very effective way of managing information risks since they can only repair some of the already occurred damage. Besides, they don't actually protect the information itself. (Yritysturva Omaisuus-, keskeytys-, vastuu- ja oikeusturvavakuutukset 2012, 16.)

2.4 Information security

As the role of information technology has become essential in today's society businesses have also become highly dependent on it. Information is one of the most important assets for many businesses, but it simultaneously makes them more vulnerable. Constant development of IT doesn't only bring new business opportunities, but causes totally unexpected information threats as well. This forces organisations to pay more and more attention on information security. (Suominen 2003, 79-81; Kuusela & Ollikainen 2005, 242-243.)

2.4.1 Definition and dimensions of information security

Information security is defined as appropriate protection of information, systems and services in normal and deviant conditions. Information security and risk management go hand in hand since information security can't be in good condition without effective risk management. Information security has three main dimensions: confidentiality, integrity and availability. Confidentiality concerns the information that is developed only for a specific organisation's use. Integrity means that information keeps a certain form through its lifespan since no information appears or disappears by itself. As for availability, it indicates that information should be available for organisation's use whenev-

er needed. It is also important to notice that the choices made concerning information security not only affect the organisation itself but also its stakeholders: suppliers, employees and customers, for instance. (Miettinen 1999, 23-28, Ovatko yrityksesi tietoriskit hallinnassa? Käytännön tietoturvallisuusopas 2001, 19.)

2.4.2 Managing information security

Since we live in the era of information technology the significance of technical solutions has to be emphasized more and more. In the future when IT applications become even more complicated it may become necessary for companies to hire a specialist for information security management. However, people are still the weakest link in information security, and the majority of information leaks, destruction and change derive from human errors. Thus loyalty, training and management should always come before technical solutions in information risk management policies. (Ovatko yrityksesi tietoriskit hallinnassa? Käytännön tietoturvallisuusopas 2001, 7, 10, 25.)

It is important to notice that changes in information are often more harmful than information leaks. Especially vulnerable are locations where information is stored: databases, for instance. It has been examined that a vast majority of Finnish companies do not notice if someone makes an invasion to their software system. This indicates that companies are either unaware of the chance of this kind of activity or haven't recognised the potential consequences. Yet external invasions may cause problems in software function and even prevent access to some crucial data. (Ovatko yrityksesi tietoriskit hallinnassa? Käytännön tietoturvallisuusopas 2001, 10, 26-27.)

In case the company operations principally rely on information its effective management becomes crucial. The organisation should establish a policy which clearly defines common practices, guidelines, induction, training, maintenance, development and procedures for malpractice. Also those organisations that are not entirely dependent on information benefit from establishment of information security practices. There are ready-made information security tools for organisations to utilise. However, it is important to note that not all the tools are appropriate for all, but they have to be selected according to the size and type of the organisation. For example, international standards for information security such as BS 7799:1995 can be utilized, but they may be too

heavy tools for medium sized enterprises as such. (Ovatko yrityksesi tietoriskit hallinnassa? Käytännön tietoturvallisuusopas 2001, 7, 16-17.)

Information security policy defines the organisation's principles and practices. Each member of the organisation commits to act according to the policy. Once the policy is clear the organisation can set an information security program which is based on the policy and careful risk analysis. The purpose of this program is to figure out the current situation and define the objectives in short and long term. Implementation of the program should be monitored and revised when needed. (Ovatko yrityksesi tietoriskit hallinnassa? Käytännön tietoturvallisuusopas 2001, 17-18.)

2.4.3 Information risks

Information risk are usually static risks thus they can only have negative or neutral effects. They are often difficult to recognize beforehand due to fast developing technology, and their abstract nature makes them even more difficult to manage. When information risks are concerned even recognition of the major risks is challenging since the consequences are difficult to estimate in financial terms. One characteristic of information risks is that they often have indirect effects in addition to the direct ones. Let's imagine a situation where a software system crashes and the fixing takes 3 hours. The direct effect resulting from this is that personnel has to use alternative (time consuming) solutions during the interruption. Later when the connection works again they have to file all the information to the system which causes indirect time loss. (Suominen 2003, 79-84.)

2.4.4 Information risk management

In recent times information risks have become prominent in the majority of organisations. Thus rough estimates are not enough any more, but the risks have to be mapped carefully. Defining adequate stage of security is usually challenging. High-level information security solutions are costly and still might not provide enough protection. The goal of information risk management is the same as that of risk management in general: to identify the major threats and take action to prevent or reduce them. However,

due to their abstract nature and assessment challenges information risks requires more careful management than risks in general. In order to find out which areas of information security should be highlighted the risks should be divided into smaller categories which makes the analysis easier and more effective. (Suominen 2003, 81.)

In this study the check-lists and other material utilized is mostly based on PK-RH website, since that material is designed precisely for Finnish SME:s. The Information Risk Chart presented on the website divides information risks in the five categories: Management, protection of information systems, actions of personnel, premises and business relationships. (PK-RH 2013, Ovatko yrityksesi tietoriskit hallinnassa? Käytännön tietoturvallisuusopas 2001 16-17.)

Another way of examining information threats is categorising them according to their nature. Miettinen (1999, 34) divides information risks in the following categories:

- Accidentally born threats
- Deliberately caused threats
- Passive threats
- Active threats
- Internal threats
- External threats
- Human-caused threats
- Nature-originated threats

Accidentally born threats usually derive from human-originated mistake or machinery malfunction. An example of accidentally born threats is an employee forgetting his cell phone to a public place. Deliberately caused threats, in turn, are always human-caused. It is question of a deliberately caused threat if someone breaks in the office and steals confidential papers, for instance. (Miettinen 1999, 34-37.)

Passive threats don't directly harm operations. An example of this could be a hacker collecting information for future use. In contrast, active threats stand for those that cause direct harm. For example, if someone would enter the company's software system and delete a massive amount of important data it would hamper the operations significantly. (Miettinen 1999, 34-37.)

Internal threats mean information security threats caused by an intern. There could be an employee leaking confidential information to a competitor, for instance. As a matter of fact, several studies show that the major threats for information security originate from inside the company. In turn, when it comes to external threats the source of threat is located outside. An example of an external threat could be a criminal finding out the user ID and password to the company's on-line bank service. (Miettinen 1999, 34-37)

The last two categories, human-caused and nature-originated threats, are easy to tell apart. It is important to note that humans cause the most significant threats for information security. What is positive in human-caused threats is that they are much easier to manage than nature-originated threats. Namely, storms, floods, earthquakes etc. are hard to forecast and get prepared for. (Miettinen 1999, 34-37.)

2.5 Knowledge –the new area of management

In spoken language information and knowledge get often mixed even though there is an essential difference between these two terms. Information can be written down and by that means utilised straight away by other people whereas knowledge is built through time and experience. Knowledge can only be possessed by humans and appears as gut feelings or insights, for instance. Also capability to speak a certain language is an example of knowledge. Languages cannot be transferred to other people by just writing them down, but the learning process is long and requires a variety of training methods. On the other hand, Spanish exercise book contains information, which helps to increase knowledge about that language. (Andrews 2007, 13.)

Knowledge can be divided into two categories: Tacit knowledge and explicit knowledge. Explicit knowledge is easy to transfer whereas tacit knowledge is difficult to communicate and its existence isn't necessarily even realised. For example, sales manager could describe characteristics of a certain customer to new salesperson by telling that the customer is tense and impulsive whereupon he should be contacted and informed regularly. These instructions are easy to take into use right away. An example of tacit knowledge could be a sales presentation. Even if there was plenty of advice given to the new salesperson in order to help him succeed it would still take much

time, practice and experience to hone his presentation skills to the same level with experienced salespeople. (Ishikawa & Naka 2007, 5-6.)

2.5.1 Knowledge risk management

Lately knowledge management has been one of the most visible themes in business administration. That is no wonder since today work is becoming less physical and more cognition- data processing- and communication-based. Knowledge has become one of the major assets in most of the companies and improvements in information and knowledge management may build great competitive advantage. However, changes never occur without risks, which is true in this case as well. During the information era knowledge has also become very short-lived. This forces businesses to constantly acquire new and transfer the existing knowledge in order to keep up with the competition. (Andrews 2007, 12; Ishikawa & Naka 2007, 32.)

The concept of knowledge risk management hasn't been there for long. Andrews (2007, 12) states that the term “knowledge risk” was introduced by BDO only ten years ago in 2003. Knowledge risks are especially related to constant employee change which leads to reinvention of the wheel, lost opportunities, doing the same job many times etc. If a key person leaves a company where knowledge risks are not managed it is likely that a major part of that person's knowledge is lost. Knowledge risk management should be started when no problems are yet at sight since under threat of lay-offs employees tend to keep the knowledge tight for themselves. This behaviour is apparent since unshared knowledge makes them all key people at the firm. (Andrews 2007, 12-13.)

Knowledge preservation requires its transfer from one person to another. Companies need to create new and replicating existing knowledge in order to keep successful. Creation of new knowledge is much more difficult to manage than replication. Lack of replication ability will eventually lead to gradual disappearing of knowledge from the firm. On the other hand, when acquiring new knowledge there is a risk that it appears irrelevant. New knowledge can also be threatened by competitors. In order to benefit from knowledge and avoid related problems knowledge risk management should an integral part of the strategy. (Andrews 2007, 14; Ståhle & Grönroos 2002.)

Knowledge risk management starts from identifying the employees who possess and need a significant amount of firm-specific knowledge in their work (knowledge about customers, suppliers, practices etc.). This knowledge can be acquired only in each specific company. For example, even a person with great professional qualifications lacks lots of firm-specific knowledge when starting in a new company. After identification phase the knowledge should be transferred from those who possess it to those who need it. None of the knowledge crucial for the firm's functions should be possessed by one person only. (Andrews 2007, 14.)

2.5.2 Knowledge preservation and transfer

Established practices for knowledge transfer could be, for example, orientation, training, meetings and co-working. In cases where knowledge transfer is aimed to take place between two employees the best means is to ask those two people work together. This kind of arrangement builds a type of master-apprentice-relationship between them. (Andrews 2007, 14.)

All in all knowledge change should be facilitated as much as possible in everyday activities since transferring knowledge from person to person is likely to have very positive effects on the firm's success. In order to facilitate knowledge change between employees attention should be paid on culture and atmosphere. Unless everybody works as a team and is open to each other it is highly unlikely to encounter knowledge change. Good relationships are not only an important key for knowledge transfer inside the company, but it may pay off to retain good relationships with ex-employees as well. These people's knowledge may appear priceless in the future. (Andrews 2007, 13.)

In small businesses “person to person” knowledge transfer works well, since the team is small, operations not very complex, and it's natural for new employees to learn by working with the experienced ones. However, when the business grows more the founders have less time for new recruits and less ability to supervise the work. If experienced employees aren't able to transfer their knowledge for the newly recruited ones the whole business may suffer. Therefore, when a company continues to grow the management should define what fundamental knowledge makes the business to prosper

(products, processes, assets, customers, risks etc.) and create information tools, such as check-lists, instructions and manuals to support that knowledge. These information tools cannot replace person to person coaching, but they can be used as a back up to facilitate the learning process. In order to keep the information tools up to date the fundamental information and knowledge should be regularly discussed and revised. (Andrews 2007, 13-14.)

3 RESEARCH METHODOLOGY

This chapter will explain how the research methods were chosen. Existing research on the field of information risk management will be dealt with and used as support for designing as functional research as possible. After that the text will present the research questions, sampling and methods in detail. Risks related to the research will be discussed in the end, as well as the uniqueness and ethical aspects of the research.

3.1 Choice between quantitative and qualitative research

It is crucial to choose the right research methods in order to gather relevant data which brings answers to the questions asked. Research can be divided in two categories: quantitative and qualitative research. Quantitative research is designed for finding out general information about masses whereas qualitative research goes more in-depth and strives for finding relations between things. Quantitative research is more often seen as the “real research” since it brings clear statistical data which can be generalised. However, quantitative research cannot tell the reasons behind the results hence it cannot exclusively be applied to research that aims at in-depth findings. All in all the best results are usually gained when the two methodologies are combined together. (Flick 2009, 24-25.)

As the goal of this study is to initiate information and knowledge risk management at company X by analysing its current risk profile and suggesting an action plan based on the findings the subject requires rather deep research. By qualitative methods it is possible to find out cause-effect-relationships for risks that have already come true or may potentially actualise in the future. The number of organisation members is small as well, which makes it easy to select the sample so that the results will respond well to the reality. (Flick 2009, 15.)

If company X had recorded frequencies or financial effects of risks that had already come true there would have been chance to present quantitative data as well and consequently support the qualitative findings. However, it appeared that such records did not exist, but all the knowledge about risk history was possessed by the organisation members. Due to the lack of quantitative data the methods used in this research are pri-

marily qualitative. However, since most of the organisation members participate in the research it is possible to generalise some of the results. Nevertheless, the results can only be generalised in company X.

3.2 Qualitative research process

Qualitative research is not as straightforward process as quantitative research. Usually the phases of research cannot be clearly arranged and separated. Therefore, after some data collection the researcher may have to go back to the first phases again. Flick (2009, 95) calls this the ”Circular model of the research process”. The phases of this research: information search, question formulation, sampling and method selection, data collection and data analysis are discussed respectively. However, it is crucial to understand that some findings may require the author to go back to the first phases again. (Flick 2009, 92-95.)

3.2.1 Information search

According to Flick (2009, 48) the importance of literature search in qualitative research should not be underestimated. In order for the research to be good quality the author should be familiar with the studied field which, in this case, is information and knowledge risk management. This information search is presented in chapter 2, Theoretical framework. Another way to benefit from existing material is scanning through similar studies which show how good quality studies have been executed and what mistakes are to be avoided. (Flick 2009, 48.)

Previous studies dealing with the same subject are used as a support for this research. Anand Singh's thesis “Improving Information Security Risk Management” focuses on enhancing information risk management methods. In his study Singh (2009, 6-7) states that even though the current methodologies provide a good framework for information risk management they still include quite many gaps. Singh sees it problematic that qualitative data is often used as the sole basis for risk management since it is difficult for decision makers to utilise that data. The goal of Singh's study is to identify the major gaps in current information security risk management methods and provide methodological improvement. (Singh 2009, 6-7.)

The findings of Singh (2009) are taken into account when proposing what kind of action company X could take in order to manage information and knowledge risks more effectively. Formal and complex statistical control over threats is likely to be too expensive for a medium-sized company X as such. However, as a rapidly growing enterprise company X will probably need more and more formal tools for control in the future.

Singh (2009, 7) states in his study that the identification of critical controls is mostly based on the author's own judgement only, since formal selection of controls is usually highly expensive. Configuration of critical controls also tends to lack specificity. Namely, risk monitoring is often solely based on qualitative methods. Security controls should include documentation of threat fruition and the subsequent financial or other consequences. Singh (2009, 8) also finds a gap in monitoring the impacts of security enhancement. It is crucial to design security enhancement processes so that their financial impacts can be monitored. That is to say, there is a chance that increased security costs total more than the initial risk actualisation costs. The fourth gap Singh (2009, 8) identifies in his thesis is the lack of dynamic adaptation to security threats. It is essential to take into consideration that organisations constantly face new threats while some of the former threats disappear. (Singh 2009, 7-8.)

Vilhelm Brag and Frida Wedefelt have also studied the field of information risk management in their bachelor thesis: Information Risk Management –A case study of major Swedish banks concerning the concept of information risk management (2004). Their thesis focuses on how the concept of information risk management was perceived within major banks in Sweden. Their goal is somewhat different compared to this study, yet the research elements are very close to each other. Namely management's risk consciousness is where the whole risk management process starts from thus management's perception of the concept is emphasized in this research as well.

Brag and Wedefelt (2004) dealt with banks which are very different organisations in comparison to company X and not the least in terms of risk management. It was interesting to see how the concept of information risk management was perceived in banks that obviously had much more voluminous risks than business gift retail companies. What Brag and Wedefelt (2004, 55-57) found out was that the managers of Swedish banks were very well aware of the information risks and they were managed funda-

mentally. There was an extensive framework established for information related practices containing, for instance, confidentiality matters and rules concerning information use, protection and storage. In fact, the practices in the studied banks seemed to be very much like those recommended in information security literature. Thus, Brag and Wedefelt's paper provides a good starting point for interviewing the management of company X. (Brag & Wedefelt 2004, 55-57.)

Literature search presented earlier in this thesis is to be used as a basis for designing the research methods. Check lists found from PK-RH website provide great support in question formulation. Those check-lists are particularly suitable for this research since they are designed exactly for the use of Finnish SMEs. As mentioned in the theoretical study risk management process should be carried out in cooperation. Therefore, the research is planned to involve management and employees of company X as extensively as possible.

When aiming at a thorough understanding of the situation it is beneficial for the author to know her research objects well. When any management-related matters of an organisation are studied it is essential to obtain comprehensive background knowledge of the organisation's functions, culture and members. This helps the researcher to formulate the right questions and approach issues in a right way. When it comes to data collection it is crucial to plan the circumstances so that the research objects feel relaxed and act and speak openly. Namely, only then will the participants give truthful answers. In this study the organisation and participants are well known by the author, since she is employed by company X as well. This helps to thoroughly plan and execute the research. On the other hand being part of the organisation is likely to have an effect on the authors objectivity. Thus, this matter is taken into consideration when planning the execution and analysis phases in detail. (Flick 2009, 16, 110-112.)

3.2.2 Question formulation

It's important to formulate the right questions since there is a potential danger of collecting a large amount of irrelevant data when qualitative research is in question. As a matter of fact, the selection of people who can bring the answers can not be made until the main questions are clear. Once the overall questions are known they should be

complemented by more specific questions. Questions should be open, but defined as carefully as possible in order to bring relevant data. There should also be room left for modifying the questions or creating new ones during the interview if unexpected information is revealed. (Flick 2009, 98.)

As the goal of this study is to initiate information and knowledge risk management at company X, the two main questions are the following:

1) What is company X's risk profile like at the moment?
2) How could the risk management be improved now and in the future?

Even though these questions require quite extensive research on risk factors it is seen important that the entire scale of information and knowledge risks is covered. Namely, the study brings more value to company X if the subject is addressed outright. I.e. this helps the management to perceive the big picture and get interested in and committed to information and knowledge risk management. It has to be taken into consideration that risk management is not a project but an ongoing process. Thus finding suitable ways for managing the risks is not the main goal of the study, but it is more important that the study encourages company X to start a long-term risk management process. That is to say, mere proposals for improvement are useless if they are not implemented in reality. Another crucial notice is that only those actions that are monitored over time can be proven beneficial.

In order to gather more specific data concerning company X's information and knowledge risks it is necessary to formulate more specific sub-questions. When investigating company X's risk profile the first step is to find out what kind of information and knowledge risks there are at the moment and how grave consequences their fruition would have. The Information Risk Chart provided by the PK-RH website is used as a support for more detailed question formulation since it covers the most typical threat factors related to information in SMEs. However, the chart doesn't cover knowledge risks thus potential threats related to knowledge are listed by the author. (PK-RH, 2013.)

The following check-list is used for identifying and assessing company X's knowledge risks in the same manner as in the Information Risk Chart.

1) Knowledge transfer
- Management
- Atmosphere
- Relationships
- Interaction
- Orientation and training of new employees

2) Knowledge preservation
- Key people leaving the organisation
- Definition of fundamental knowledge
- Transforming knowledge into information

The second main question of this study, “how could company X's information and knowledge risks management be improved now and in the future”, is also divided into more specific sub-questions in order to find the most suitable solutions for this case. First of all it is important to ask how information and knowledge risks are managed at company X at the moment. Sub-questions concerning that are the following:

1) Has company X established some kind of information and knowledge risk management programme and what does it specifically include?
2) What kind of formal and informal action have been taken in terms of information and knowledge risk management?

Knowledge about the current state of affairs at company X is crucial when progressing to the actual risk management methods. Questions related to this are the following:

1) What kind of action should be taken under each identified risk?
2) How could the overall practices be improved in order to reduce costs resulting from risks?

3.2.3 Sampling and method selection

Since the author herself is a member of the organisation she is constantly observing what is going on in the company. Because of this it is natural that ethnography is used as one research method in this study. The advantages of using ethnography in this case are the researcher's easy access to the social settings studied and possibility to use a comprehensive sample due to natural interaction with all the other group members. Also the open atmosphere at company X provides very suitable settings for ethnography. Common problems in ethnography are how to choose what to observe and how to know the frequencies of different events. In this case these problems can be mitigated since the ethnographer has quite much knowledge of the activities taking place at company X. This facilitates the selection of actions on which to focus. When it comes to estimating frequencies rather reliable conclusions can be drawn from long-term observation. However, it has to be considered that being a member of the studied organisation may also cause inability to see the forest for the trees. (Bryman & Bell 2011, 440-460; Flick 2009, 232.)

Participant observers can take different roles in their research varying from total involvement to full detachment. Since in this study the researcher is a full member of the studied group the role of hers is chosen to be complete participant which indicates very high involvement. In complete participation the other members are unaware of the observation actions. Thus complete participant is a covert observer. When the observing actions are unknown by the other group members the gathered data is reliable. Namely, the research objects don't know they are observed. However, it is important to take ethical aspects into consideration when reporting the findings. Covert observation seldom brings enough data since the ethnographer has to keep low profile in order not to be uncovered. Because of this interviews are used for complementing the ethnographic method. (Bryman & Bell 2011, 450, 454.)

After the observation period the information and knowledge risks will be identified and assessed in detail in a group-discussion-type interview between employees, since most of the risk management material suggest that risk identification and assessment process should be executed in cooperation. In order for the sample to correspond the entire population it is designed to include approximately 50% of the employees with different roles in the company: salespeople, secretaries and purchasers. The manage-

ment is not included to the group discussion since the presence of the CEO might affect the openness of personnel's conversation. (PK-RH 2013; Suominen 2003, 58.)

Company X's financial manager is interviewed separately since she encounters information risks that are very different to those faced by other employees. It can be assumed that some of the largest information risks concentrate specifically on finance. Also knowledge risks are expected to be large when it comes to financial manager's post, since she is almost exclusively liable for the company's finance.

Since some of the issues presented on the information risk check list can only be examined by discussing with the management, the CEO is interviewed as well. These issues include the management's attitude towards and awareness of information risks, contract policies, external assistance and actions for enhancing protection, just to mention a few. The interview is carried out after the other interviews since by that means the facts revealed in the first interviews can be used as a basis for final question formulation.

3.3 Risks

When doing qualitative research the probability of bias has to be taken into consideration and avoided as much as possible. In this case it is important to find out if there has been risk management action taken before and if some of the interviewees are part of a risk management group, for example. Those group members would probably state that they have been able to prevent the most significant risks. On the other hand those who are not part of the risk management group would probably give more objective views of the situation.

Qualitative research tends to be time-consuming. That is taken into account when planning the schedule and design of execution and analysis phases. Interviews will be designed so that not much irrelevant data is collected. Instead, the questions will be formulated so to bring answers to the core questions in an effective way. Interviews are scheduled as well, since no time of the participants and the company should be wasted.

One of the biggest limitations related to this research is that the interviewer is part of the same working community with the interviewees. This may have an effect on the objectivity of the research partly because the interviewer tends to be affected by her own opinions and partly because she is likely to influence the objectivity of interviewees' answers. In order to get as objective data as possible the interviewees will be selected from those who are not so well known by the interviewer. Additionally, the interviewer will avoid questions and body language that might lead the interviewees towards certain opinions. In order to avoid personal opinions in the analysis phase, the interviewer will discuss the data with a third, fully objective, party.

3.4 Uniqueness

Each research aims at bringing new information. The goal of this study is to bring new and useful information to company X in the field of knowledge and information risk management. What makes this study unique is that it combines information and knowledge risks together whereas most of the previous studies focus on information risks only. All in all there is only little research made of knowledge risks, but in the author's opinion information and knowledge should be bound together. Namely, many businesses suffer from inability of converting information into knowledge and vice versa. Another thing making this paper unique is that it is the very first risk study conducted for company X.

3.5 Ethical aspects

This study follows the ethical principles stated in Business Research Methods written by Alan Bryman and Emma Bell (2011, 126-150). Thus, the research will not cause any physical or mental harm to interviewees. The management of company X as well as the participants have been asked a consent for the interview. Confidentiality issues will be clarified for the participants. Privacy of the participants will not be hurt in this study nor will any data be used for deception. (Bryman & Bell 2011, 126-150.)

4 FINDINGS

In this section the author will describe in detail how the research was executed in reality and what kind of results it gave. The findings are reported in the same order as the data was collected: Ethnographic findings at first and interviews after them.

In order to make this study easier for the reader to follow the research questions are repeated once more. The main questions which this study aims to answer are stated below:

1) What is company X's risk profile like at the moment?
2) How could the risk management be improved now and in the future?

Finding out the most significant risk factors requires identification and assessment of company X's entire information risk field. This process is facilitated by using the information risk chart provided by PK-RH website (figure 5).

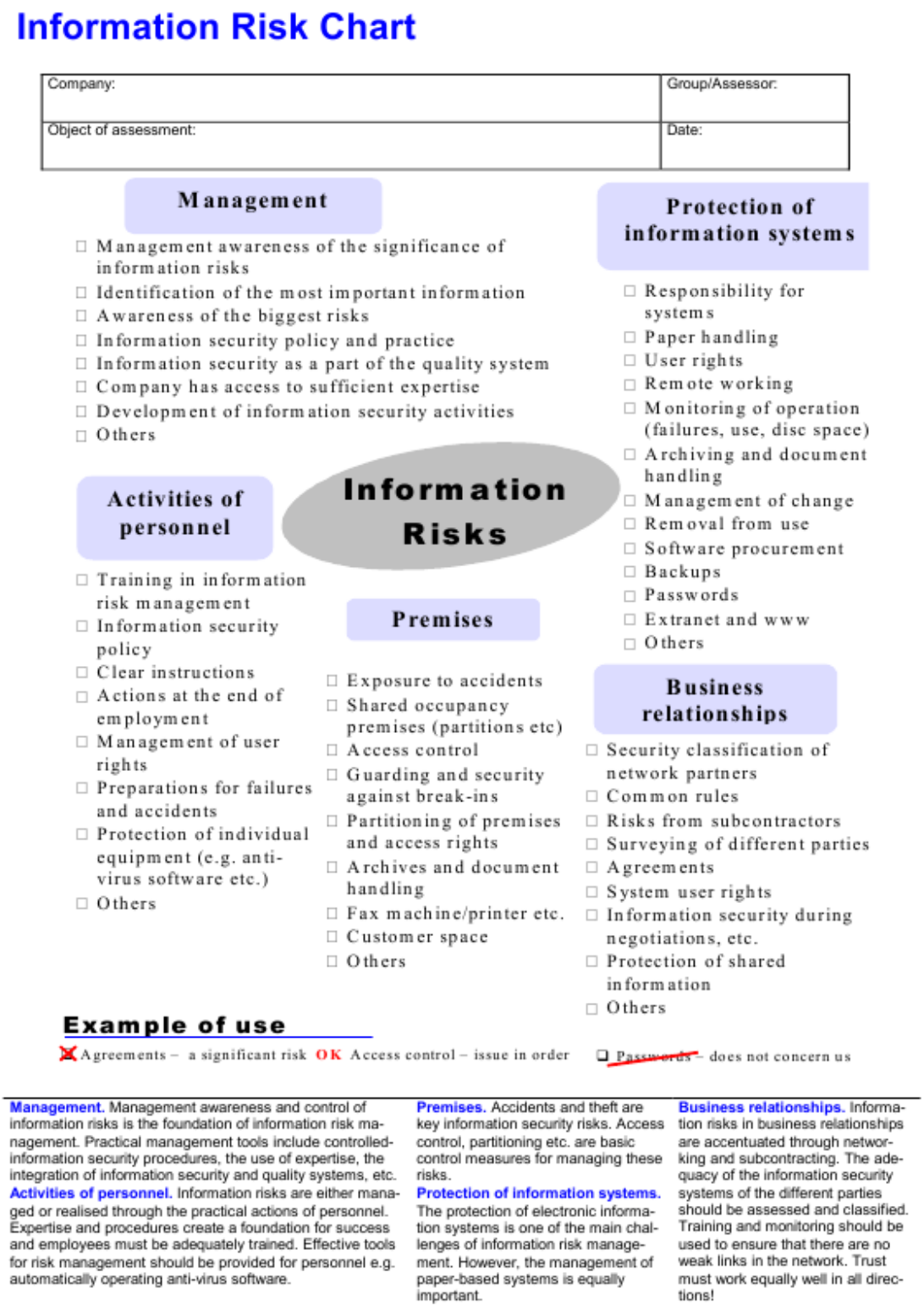

FIGURE 5. Information Risk Chart (PK-RH 2013)

Since no tools for knowledge risk assessment were found from secondary sources the author designed a separate check list for that. The areas related to knowledge risks are listed in a similar manner than shown in the Information Risk Chart.

Knowledge Risk Check-list:

1) Knowledge transfer
- Management (awareness, interest, skills, practices)
- Atmosphere
- Relationships
- Interaction
- Orientation and training of new employees

2) Knowledge preservation
- Key people leaving the organisation
- Definition of fundamental knowledge
- Transforming knowledge to information

As the first main question focuses on examining company X's current risk profile, the second main question “How could company X's risk management be improved now and in the future?” aims at providing company X with the tools for information and knowledge risk management in practice. The questions formulated for finding out those tools are presented below once more.

1) What kind of action should be taken under each identified risk?
2) How could the overall practices be improved in order to reduce costs resulting from risks?

4.1 Ethnographic findings

As mentioned earlier the ethnographic research method used in this study is covert observing. The indirect observation period can actually be defined having begun once the author started working for company X in the beginning of April in 2012. Even though the author didn't know about this research during the first eight months in company X she was inevitably observing the company environment and operations all the time. The observation conducted by a newcomer is always more valuable and effective in comparison to observation carried out by an intern. Namely, people tend to become blind for action taking place around them when they get used to it.

This page is intentionally left blank

This page is intentionally left blank

This page is intentionally left blank

This page is intentionally left blank

This page is intentionally left blank

This page is intentionally left blank

This page is intentionally left blank

This page is intentionally left blank

This page is intentionally left blank

This page is intentionally left blank

This page is intentionally left blank

This page is intentionally left blank

This page is intentionally left blank

This page is intentionally left blank

This page is intentionally left blank

4.3 Outline

Once the substantial risk factors were identified by observation and interviews they were assessed in order to point out the most dangerous risks. The assessment was executed as described earlier in this text –by defining a numerical value of severity and frequency for each risk and multiplying these numbers by each other. Four-step assessment scale (table 3) was determined being the most suitable scale for this purpose since information and knowledge risk assessment is very challenging to assess with high accuracy. This is due to the risks' abstract nature and lack of precise risk documentation from previous years. As there was not such documentation available there was no other chance than to settle for relatively rough estimations. However three-step scale would have been too rough in this case since the variations in the frequency and consequences of different information and knowledge risks are high. (Suominen 2013, 83-84.)

The assessment of company X's information and knowledge risk tolerance is shown risk by risk in table 4. Severity and frequency are given numerical values from one to four, one standing for slightly harmful or highly unlikely, two for somewhat harmful or unlikely, three for harmful or somewhat likely and four for extremely harmful or likely risks. The frequency scale is proportioned to the time of 15 years which the company had been in operation thus highly unlikely risks were defined as those taking place approximately once in every twenty years, unlikely risks once in every five years, somewhat likely risks once in a year and likely risks once in a month. The Severity scale, in turn, is defined based on the CEO's estimations concerning the seriousness of financial losses. Accordingly, in the case of company X slightly harmful consequences would correspond losses less than 20 000€, somewhat harmful consequences 20 000 – 100 000€, harmful consequences 100 000 – 500 000€, whereas extremely harmful consequences would signify losses greater than 500 000€.

TABLE 3. Assessment scale for information and knowledge risks at company X

Likelihood of the risk	**Severity of the risk**			
	1 Slightly harm-ful (<20 000€)	2 Somewhat hrmful (20 000–100 000€)	3 Harmful (100 000–500 000€)	4 Extremely harmful (>500 000€)
1 Highly unlikely (once in 20 years)	1 Very trivial	2 Trivial	3 Tolerable	4 Moderate
2 Unlikely (once in five years)	2 Trivial	4 Tolerable	6 Moderate	8 Substantial
3 Somewhat likely (once in a year)	3 Tolerable	6 Moderate	9 Substantial	12 Intolerable
4 Likely (once in a month)	4 Moderate	8 Substantial	12 Intolerable	16 Catastrophic

This page is intentionally left blank

This page is intentionally left blank

5 RECOMMENDATIONS

In this chapter the risks that were identified and assessed in chapter 4 will be addressed one by one, and potential management methods and actions suggested. After that the situation will be analysed as a whole and essential risk management actions and schedules proposed. These recommendations will subsequently be presented to company X's management that has the authority to choose which proposals will be implemented in reality. Company X's management will also be proposed an information and knowledge risk programme for continuing risk management in the future as well. (Suominen 2003, 30.)

As stated earlier in this paper, there are four different risk management methods the first two of which belong to risk control and the last two to risk financing procedures:

- Risk avoidance (control)
- Risk reduction/sharing (control)
- Risk transfer (financing)
- Risk keeping (financing)

These risk management methods are used as a basis for determining the most suitable action to be taken under each risk. Since each risk effect has also a cause it is the causes that have to be focused on when the aim is to impact the effects. Some causes can and should be totally avoided whereas the removal of certain causes may become more expensive than the costs deriving from risk actualisation. Some risks may have positive effects as well, but information risks cause usually only harm or no harm thus most of them belong to the category of static risks. (Suominen 2003, 98, 79; PK-RH 2013.)

Company X's most significant information and knowledge risks are presented in the previous paragraphs. Risk management should start from the most dangerous risks since their actualisation would cause much harm. Thus the risks will be reviewed in the following table starting from the substantial ones and then proceeding to the moderate, tolerable and trivial ones respectively. The risks are divided in two tables the first of which (table 5) includes information risks and the second (table 6) knowledge risks. This division facilitates the specification of suitable risk management actions

since most of the management actions can be applied to several risks within one risk category. (PK-RH 2013; Suominen 2003, 83.)

This page is intentionally left blank

This page is intentionally left blank

This page is intentionally left blank

This page is intentionally left blank

As it can be noticed from the tables above most of the means for risk reduction would affect plenty of risks at the same time. This aspect has to be taken into account when defining the urgency of certain risk management actions. Namely, improving only one thing may reduce the likelihood or frequency of several risks at the same time. The tables also show that most of the potential risk management actions belong to the reduction category, which indicates that the risks cannot be totally avoided. When information risks are in question their absolute elimination is usually impossible due to the major role of unintentional actions and human errors within cause factors. Knowledge risks, for their part, are quite challenging to avoid and impossible to transfer because of their abstract nature. (Suominen 2003, 80.)

It appears that company X has seven substantial information and knowledge risks altogether. Actualisation of more than one or two substantial risks could hardly be tolerated. Therefore, it is crucial to start improving the firm's tolerance for these risks right away. Four of the substantial risks belong to the category of information risks whereas three of them are knowledge risks. These two categories require quite different management actions hence they will be discussed separately.

5.1 Methods for information risk management

When examining the information risk table some of the suggested management actions appear to recur under several risks. The four substantial risks presented on the first rows of the table could be significantly reduced by only a couple of measures. These measures also appear to affect most of the less dangerous risks. What is even better from company X's point of view is that most of these measures are quite inexpensive and easy to implement.

This page is intentionally left blank

This page is intentionally left blank

This page is intentionally left blank

This page is intentionally left blank

5.2 Methods for knowledge risk management

The research detected five knowledge risks at company X three of which belong to the category of substantial risks, one to moderate risk and only one to tolerable ones. Thus it is highly recommended for company X to take prompt action in order to reduce these risks. It has to be noted, however, that knowledge management is not any project, but it should be permanently integrated in the management. It is imperative, yet challenging, to get each member of the organisation involved in the process. (Atwood 2009, 1-2.)

This page is intentionally left blank

This page is intentionally left blank

This page is intentionally left blank

6 CONCLUSION

Information and knowledge risk management in company X was chosen as a subject for this thesis since the firm's operations were almost entirely based on communication. Another reason behind the need for improving information and knowledge risk management were the constantly increasing challenges in that area, such as development of technology, employees changing work place more often than in the past and accurately filed customer information becoming prerequisite for success. Accordingly, the goal of this study was to initiate information and knowledge risk management at company X by analysing its current risk profile and suggesting an action plan based on the findings.

The theoretical framework of risk management, information security, knowledge management and qualitative research provided a good starting point for primary data collection. The research was executed by qualitative methods since it aimed at pointing out cause-effect relationships and finding out solutions for existing problems. Quantitative data concerning risk actualisation in the past would have been useful as well, but unfortunately there wasn't such data available. The research was started by covert observing which was continued for several months. The ethnographic findings proved valuable and ample, but some especially management-related issues required adjustment thus the management and representative of company X's information security service provider were interviewed individually. The overall risk profile was also discussed and assessed in a group interview with six staff members making approximately half of the entire personnel.

This page is intentionally left blank

The design, implementation and results of this study are not flawless, especially because it was the first risk management study conducted for company X. Even though many of the significant risks were identified, it is still possible that some risks remained unnoticed due to the great number risks out there. But as mentioned earlier, risk management is an ongoing process. Thus it is up to company X to continue the process that was started by this study. This paper also provides a good basis for managing other risk categories at company X.

All in all, the ultimate gain of this thesis lies on awaking the interest of company X's management on the subject of risk management. As competitive advantage is what matters the most in corporate gift business, awareness of the risk management may prove to be a decisive asset. Information and knowledge management are also relatively new fields of administration making the related threats and possibilities notable. Thus competent management of related risks is likely to bring great competitive advantage in the future.

LIST OF REFERENCE

Andrews K. 2007. Knowledge risk and knowledge for growth: Two challenges of growing businesses. Growing Businesses Summer 2007. 12-14.

Atwood C. 2009. Knowledge Management Basics. ASTD Training Basics ASTD Press.

Brag V. & Wedefelt F. 2004. INFORMATION RISK MANAGEMENT -A case study of major Swedish banks concerning the concept of information risk management. Göteborg University: School of Economics and Commercial Law. Department of Business Administration / Industrial and Financial Management. Bachelor's Thesis.
Bryman A. & Bell E. 2011. Business Research Methods. USA: Oxford University Press

Flick U. 2009. An Introduction to Qualitative Research. London: SAGE Publications Ltd.

Ishikawa A. & Naka I. 2007. Knowledge Management and Risk Strategies. NJ, USA:World Scientific Pub Co.

Koroma J. 2001. Ovatko yrityksesi tietoriskit hallinnassa? Käytännön tietoturvallisuusopas. Helsinki. Teollisuuden ja Työnantajain Keskusliitto.

Kuusela H. & Ollikainen R. 2005. Riskit ja Riskienhallinta. Tampere University Press. TUP.

Liiketoimintaa Turvallisesti -Kansallinen strategia yritystoiminnan turvallisuuden parantamiseksi. 2012. Työryhmämuistio 30/2012. Helsinki. Sisäasiainministeriö.

Miettinen J. E. 1999. Tietoturvallisuuden johtaminen - näin suojaat yrityksesi toiminnan. Kauppakaari.

Newton C. Factors Influencing Employee Commitment. Demand Media, Inc. Ehow. Read. 20.6.2013. http://www.ehow.com/.

Pérez M. Á. M. Aon Risk Services. Fundación Mapfre. 2010. Risk Management tools: reduction of the Total Cost of Risk. Read 17.6.2013. http://www.fundacionmapfre.org/fundacion/es_es/default.jsp

PK-RH-Foorumi. 2000-2009. Pk-yrityksen riskienhallinta. Read 5.9.2013. http://www.pk-rh.fi/index.html.

Punkka A-J. 2011. Tapani kotimaisen myrskyhistorian raskaaseen sarjaan. Myrskyvaroitus.com. Read 12.7.2013. http://www.myrskyvaroitus.com/site/index.php.

Singh A. 2009. Improving Information Security Risk Management. University of Minnesota. Faculty of Philosophy. Doctoral thesis.

Ståhle P. & Grönroos M. 2002. Knowledge management: tietopääoma yrityksen kilpailutekijänä. Helsinki: WSOY.

Suominen A. 2003. Riskienhallinta. Helsinki: WSOY.

The Australian National Audit Office. 2012. Example risks and risk treatments: Contract management phase. Read 16.6.2013. http://www.anao.gov.au/.

Wheelhouse Advisors LLC. The ERM Current™. 2009. Reputation Risk Takes Center Stage. Read 6.6.2013. http://wheelhouseadvisors.com/

Wiley J. & Sons. 2006. How to Answer CEO Questions about Knowledge -extract from Andrews, Kate: DNA@ work. Read 16.7.2013. http://www.knowable.com.au/.

Yritysturva Omaisuus-, keskeytys-, vastuu- ja oikeusturvavakuutukset. 2012. Tuote-esite. Helsinki. Keskinäinen Vakuutusyhtiö Fennia.