LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Development of Security Risk Assessment in an IT and Business Consulting and Outsourcing Company

Kaisa Cullen

2018 Laurea

Laurea University of Applied Sciences

Development of Security Risk Assessment in an IT and Business Consulting and Outsourcing Company

Kaisa Cullen
Degree Programme
Security Management
Bachelor’s Thesis
May, 2018

Laurea University of Applied Sciences
Degree Programme in Security Management
Bachelor's Thesis

Abstract

Kaisa Cullen

Development of Security Risk Assessment in an IT and Business Consulting and Outsourcing Company

Year 2018 Pages 42

Risk management is a systematic and continuous approach to considering risks that organisations face. Its ultimate goal is to bring value. Risk assessment is a part of the risk management process. It includes the phases of risk identification, risk analysis, and risk evaluation.

The objective of this functional thesis was to determine how to best develop the local risk assessment methods of the case company. The purpose was that those, who represent their sub-business units, can assess security risks in an efficient and reliable manner. The security lead can use these results to make an accurate and realistic risk assessment of the whole business unit.

Literature review and participant observation were used to collect data. The literature review includes both general works in the field of risk management and company-specific material. Participant observation was performed throughout the process in workshops and other means of communication. Content analysis was exploited to analyse the collected data.

The concrete outcome of this thesis is two products, a risk assessment tool and a guide to support risk assessment. The new tool is simple to use and highly automated in terms of calculations. It has a clear layout, colours, and summarising tables. The possibility of erroneous use has been eliminated as far as possible. The Security Risk Guide provides very concise explanations for the threats identified in the risk assessment tool and lists protective measures. It also contains questions to support risk assessment.

It can be concluded that the output of this thesis meet the set objectives and that they help the security lead in making the final risk assessment of the whole business unit. The feedback has been positive. Especially the possibility to identify and report new threats has been considered an improvement. The risk assessment process could be developed further by providing more training for risk coordinators and by increasing cooperation between business units.

Key words: Risk, Risk analysis, Risk assessment, Risk management, Security

Laurea-ammattikorkeakoulu
Turvallisuusalan tradenomi
(AMK)

Tiivistelmä

Kaisa Cullen

Development of Security Risk Assessment in an IT and Business Consulting and Outsourcing Company

Vuosi 2018 Sivumäärä 42

Riskienhallinta on organisaatioiden järjestelmällistä riskeihin varautumista. Sen perimmäinen tavoite on tuoda yritykselle lisäarvoa. Riskien arviointi on osa riskienhallintaprosessia. Siihen sisältyy seuraavat vaiheet: riskien tunnistaminen, riskianalyysi ja riskien merkitysten arviointi.

Tämän toiminnallisen opinnäytetyön tarkoitus oli selvittää, miten paikallisia riskien arvioinnin menetelmiä voisi parhaiten kehittää yrityksessä. Tavoite oli, että liiketoimintayksikköjen riskikoordinaattorit pystyvät arvioimaan riskejä tehokkaasti ja luotettavasti. Turvallisuuspäällikkö hyödyntäisi näiden arvioiden tuloksia tehdessään turvallisuusriskien arvioinnin koko Suomen liiketoimintayksiköstä.

Tiedonkeruumenetelminä on käytetty kirjallisuuskatsausta ja osallistuvaa havainnointia. Tietoperustaan sisältyy sekä riskienhallinnan yleisteoksia että toimeksiantajan laatimaa sisäistä materiaalia. Osallistuvaa havainnointia tehtiin pitkin kevättä muun muassa riskityöpajoissa. Kerättyä aineistoa analysoitiin sisällönanalyysin avulla.

Opinnäytetyön tuloksena syntyi kaksi produktia: riskienarvioinnin työkalu ja opas. Uusi työkalu on yksinkertainen käyttää, ja siinä on hyödynnetty laskentakaavoja. Siinä on selkeä rakenne ja värit, ja arvioinnin tiivistetyt tulokset päivittyvät työkalun ylälaitaan. Virheellisen käytön mahdollisuus on estetty niin pitkälle kuin se on mahdollista. Opas sisältää ytimekkäät kuvaukset eri uhkakuvista ja keinot niiltä suojautumiseen. Oppaassa on lisäksi pohdintaa tukevia kysymyksiä.

Voidaan todeta, että opinnäytetyön aikana tehdyt produktit ovat toimeksiannon mukaisia ja että ne tukevat Suomen turvallisuuspäällikköä riskien arvioinnissa. Lopputuotokset ovat saaneet positiivista palautetta. Erityisesti mahdollisuutta tunnistaa ja merkitä uusia riskejä on pidetty hyvänä uudistuksena. Kehittämisehdotuksena esitetään, että toimeksiantaja voisi parantaa riskienarviointiprosessiaan lisäämällä riskien arvioinnissa mukana olevien koulutusta sekä yhteistyötä liiketoimintayksikköjen välillä.

Avainsanat: Riski, Riskianalyysi, Riskienarviointi, Riskienhallinta, Turvallisuus

Table of Contents

1 Introduction 6
1.1 Objectives and Scope 6
1.2 Key Concepts 7
2 Case Company...8
2.1 Organisation 8
2.2 Security Risk Management..9
2.3 Security Risk Assessment 9
3 Methodology.. 11
3.1 Qualitative and Functional Thesis 11
3.2 Methods.. 12
4 Risk Management 14
4.1 Security 14
4.2 Organisational Risks 15
4.3 Corporate Governance and Enterprise Risk Management............................ 16
4.4 Risk Management Process 17
4.5 Risk Assessment 21
5 Process 23
5.1 Planning and Preparing 24
5.2 Execution and Finalising 25
6 Results... 26
6.1 Products 26
6.2 Observations and Response 29
7 Discussion... 31
8 Conclusions and Self-Assessment 32
References 35
Figures 38
Tables... 38
Appendices... 39

1 Introduction

Uncertainty about the future is present in our everyday life. We cannot know the outcome of our own actions or events that we have no control of. Yet, we have to make decisions. This poses risks. Organisations that want to thrive have to take calculated risks and accept the possibility of failure (Hopkin 2017, 45). In our everyday life, as individuals, we rely on common sense, knowledge, experience, and even our instincts (Merna & Al-Thani 2010, 7). However, successful organisations should have a well-established and structured approach to risk management. This will help organisations in defining their strategy, reaching objectives, and making the right decisions. (SFS-ISO 31000:2018, 5.) Moreover, risk management should not be seen as merely a question of compliance. Rather, it supports organisations in identifying opportunities to expand, make profit, and gain good reputation, among other things. (Burns-Howell, Cordier & Eriksson 2003, 67.)

The writer of this thesis was employed by the case company in January 2018 as a Global Security Trainee. The company has developed an enterprise-level risk assessment tool which is used for annual risk assessments. It is a complicated, Excel-based tool which is best suited for reporting the final risk assessment results for the entire business unit. The need for a new risk assessment tool and supporting material for local use was established in the beginning of the employment. Thus, it was decided that, after the initial training period, a functional thesis would be carried out to develop and implement a new tool and a short guide for the purpose of risk workshops. Naturally, a regular presence on the company premises and access to useful resources offered an excellent starting point for this functional thesis. Also the timeframe was suitable: risk assessment for the fiscal year of 2019 was to be carried out in the spring.

In this chapter, the objectives and the scope of this thesis are determined and some key concepts to support the reader are provided. The second chapter introduces the case company and describes its risk management and risk assessment approaches. The third chapter is dedicated to methodology, and the fourth chapter provides a theoretical framework about risks in general and risk management in particular. In the fifth chapter, the whole thesis process is explained, and the sixth chapter presents the results. The seventh chapter entails discussion. The final conclusions, including the writer's own assessment of the thesis, are in the eight chapter.

1.1 Objectives and Scope

The objective of this functional thesis was to determine how to best develop the local risk assessment methods of the case company. If the new methods prove successful, they can be implemented in future risk assessments also in other business units. The purpose was that those, who represent their sub-business units, can assess security risks in an efficient and reliable manner. With the help of these results, Finland's security lead will be able to make an accurate and realistic risk assessment of the whole business unit. The final results will be put into the original enterprise-level risk assessment tool which will then be approved and sent to the headquarters abroad for final instructions and recommendations. Participants of the risk workshops will be given feedback also on a local level.

The identified research question is:

> What kind of local risk assessment method would support the security lead in assessing security risks?

This research paper will first cover risk management on a theoretical level and then the first stage of the case company's security risk management process, which is the risk analysis, on a more practical level. The scope of the risk analysis is eight sub-business units in Finland and a sub-business unit in Estonia. Only risks related to security are included in this risk analysis. However, the resulting tool can be adopted for other risk areas. The final instructions and recommendations from management from the headquarters, in other words the response, monitoring, and final reporting stages, will be excluded from this thesis.

1.2 Key Concepts

Here are definitions for the most relevant terminology in this paper.

Risk, according to the ISO 31000 standard (2018, 6), is the effect of uncertainty on objectives. Here, an effect is considered a deviation from what is expected. Juvonen et al. (2014, 8-10) conclude that there are three factors connected to risk: the uncertainty, the expectations, and the scale and the seriousness of an event. The Institute of Risk Management sees risk as a combination of the probability of an event and its consequences which can be either positive or negative (A Risk Management Standard 2002, 2).

Risk analysis is part of the risk assessment process. Its goal is to understand the nature of risk and to find the appropriate risk levels. The factors to consider are uncertainties, risk sources, consequences, likelihood, events, scenarios, controls, and how effective these controls are. (SFS-ISO 31000:2018, 16.)

Risk assessment is a process that has typically three main phases: risk identification, risk analysis, and risk evaluation (Juvonen et al. 2014, 18). Risk assessment in an organisation can be a top-down or a bottom-up exercise depending on whether it is undertaken by the management level or the local business unit level (Hopkin 2017, 120).

Risk management is comprised of coordinated actions, the goal of which is to guide and control risk activities in an organisation (SFS-ISO 31000:2011, 13). It is a process that helps organisations understand, evaluate, and take actions on risks. The aim is to increase the probability of success and to decrease the likelihood of failure. (Hopkin 2017, 46.)

Security can be defined as freedom from danger. It is safety against internal and external threats. Typically it refers to being safe from intentional, criminal activities. (OED 2018.) The concept of security is broad, multidimensional, and dependent on the context it is used in. Security can be further classified into categories of, for example, physical security, information and computing security, criminology, and business continuity management. (Brooks 2009, 1-8.)

2 Case Company

This chapter will first discuss the case company in general. Then, the constitution and the structure of the organisation are explained. Finally, the case company's current risk management approach and risk assessment process are described.

2.1 Organisation

The case company is an IT and business consulting and outsourcing company which was founded in the 1970s in Northern America. Now a global organisation with tens of thousands of professionals in hundreds of locations and a revenue of close to seven billion Euros (2017), the company helps its clients with their digital transformation by offering end-to-end solutions. The case company has expertise in several industries, including banking, communications, transportation and logistics, manufacturing, and utilities. It has clients both in public and in private sectors. (Internal material about the case company 2018.)

The case company strives to create an environment in which its employees enjoy working together for a company they can be proud of. This idea was formulated back in the 1970s when the company was founded. It is supported with a vision, a mission, and values that together form the company constitution. The company vision is to be a leader in its own field and to help its clients succeed. Its mission is to provide outstanding quality, competence, and objectivity through best services and solutions to fully meet clients' expectations. The principle values that guide all the employees and shareholders are partnership and quality, objectivity and integrity, intrapreneurship and sharing, respect, financial strength, and corporate social responsibility. (Internal material about the case company 2018.)

The global organisation is divided into strategic business units and further to business units. The business unit of Finland and Estonia is part of the Northern Europe strategic business unit which is made up of eight countries. Every business unit has sub-business units which are formed on the basis of their business operations. In Finland, the company has close to 20 locations and employs almost 4 000 people. In Estonia there are two locations, and together they employ over 200 people. (Internal material about the case company 2018.)

2.2 Security Risk Management

The company has divided risks into seven areas: 1) winning business, 2) operational excellence, 3) member risks, 4) security risks, 5) compliance risks, 6) strategic business unit and corporate strategic risks, and 7) nascent risks. The risks in the fourth area, security risks, are included in the scope of this thesis. The company's security risk management process is an essential part of the company's security management framework, and it is aligned with the Enterprise Risk Management (ERM) approach. The process is owned by the case company's global security organisation. It is a continual process which identifies, prioritises, and responds to risks. The company's risk management is a joint, global effort to ensure comprehensible evaluations and cost-efficient solutions. The goal is to protect the organisation, its assets, and its operations by supporting the management in making the right decisions. (Internal material about risk management 2018.)

Security risks are further divided into four domains: Protecting sensitive and critical information, Protecting critical business infrastructure, Safeguarding physical assets and facilities, and Protecting people. Several threats have been identified for all these domains. The guiding principles are as follows: 1) Common solutions for the organisation are preferred, 2) The global chief information officer is responsible for designing IT solutions for technical controls, 3) Business units are accountable for their risks and responsible for their risk mitigation efforts, and 4) Adjustments in business units are made based on identified technical and operational risk events and trends. (Internal material about risk management 2018.)

The risk management process has three main stages: risk analysis, risk response, and risk monitoring and reporting. The annual risk assessment process is part of the risk analysis stage. Its main goal is to find common solutions for the most significant risks. The assessment process utilises a bottom-up approach. This means that the risk assessment work begins at the sub-business unit level and finishes at the enterprise level view on required risk mitigation actions. The risk assessment process is initiated in workshops where the business unit's security lead acts as a facilitator and subject matter experts provide the input. An enterprise-level risk assessment tool is used for this purpose. The outcome is a business unit security risk assessment draft. (Internal material about risk management 2018.)

2.3 Security Risk Assessment

In the risk analysis phase, potential security risks are identified using different sources. After the potential risks have been identified, risks are assessed to get an accurate picture of the risk exposure and how it relates to the case company's risk tolerance. Security events are followed up on and resolved on an ongoing basis. In the annual risk assessment, risk levels are identified and appropriate responses determined using a bottom-up approach. An enterprise-level risk assessment tool is used for this purpose. There are five risk levels: very low, low, moderate, high, and very high. They are determined using the model presented in Figure 1. (Internal material about risk management 2018.)

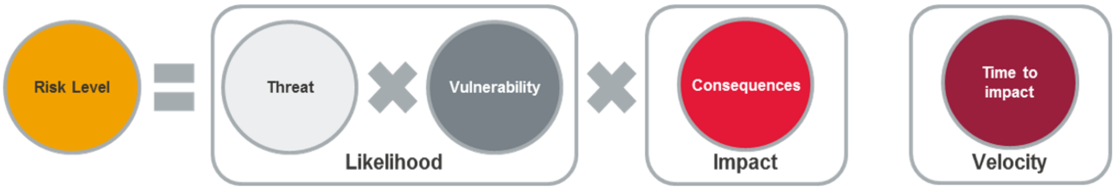


Figure 1: The model for calculating risk levels (Internal material about risk management 2018)

Identified threats to security fall under four risk domains: 4.1 Protecting sensitive and critical information, 4.2 Protecting critical business infrastructure, 4.3 Safeguarding physical assets and facilities, and 4.4 Protecting people. The number four refers to the area of security risks, and the second number to the domain within the area of security risks. The identified threats for 4.1 are equipment, media, documents theft or loss, human error, hacking, system sabotage or system intrusion, insider threat, malware, sniffing or tampering of communications, and social engineering attacks. The risk domain of 4.2. covers the threats of human error, hacking, system sabotage or system intrusion, insider threat, malware, denial of service attack, technical infrastructure or application failure, criminal or interpersonal threats or violence including collective actions, physical threats and hazards including transportation and traveling, and natural disasters. The threats for 4.3 are criminal or interpersonal threats or violence including collective actions, physical threats and hazards including transportation and traveling, and natural disasters. The risk domain of 4.4 includes the threats of criminal or interpersonal threats or violence including collective actions, physical threats and hazards including transportation and traveling, natural disasters, and medical or health issues. Many of these identified threats are connected to information technology. (Internal material about risk management 2018.)

Every threat has also a type: deliberate, accidental, or natural. Threats have five possible levels: doubtful (1), uncertain (2), anticipated (3), expected (4), and confirmed (5). The threat level is determined on the basis of how likely the threat is to occur or be initiated. There are five vulnerability levels: very low (1), low (2), moderate (3), high (4), and very high (5). These levels are based on the effectiveness of existing security controls and how quickly the company can recover from a risk that has occurred. (Internal material about risk management 2018.)

The resulting likelihood figure estimates the probability of a threat exploiting a vulnerability. It has five levels: slight (<10%), not likely (10-30%), likely (30-60%), high likely (60-90%), and expected (>90%). Impact, which can be either direct or indirect, describes the consequences of a risk for the company as shown in Table 1 (Internal material about risk management 2018):

Impact Level		Description
5	Critical	Loss of ability to achieve company’s objectives and sustain ongoing operations
4	Very important	Materiality reduced ability to achieve company’s objectives
3	Important	Moderate impact on the achievement of company’s objectives
2	Low importance	Disruption of normal activities with limited effect on the achievement of company’s objectives
1	No impact	No material impact on the achievement of company’s objectives

Table 1: The five impact levels and their descriptions (Internal material about risk management 2018)

Velocity is an estimation of how quickly the impact of the risk affects the company. It does not have an effect on the risk level as such, but instead it helps in planning and prioritising risk mitigation efforts. Velocity has three levels: high (less than three months), medium (3-12 months), low (more than 12 months). Most of the risks in the case company have a high velocity level; in other words, risks affect the company in under three months. There are three main outcomes of the annual risk assessment process: an Enterprise Security Annual Report to support strategic planning, Enterprise Security Plans to address risks, and Business Unit Security Plans to mitigate local risks. (Internal material about risk management 2018.)

3 Methodology

The strategy applied to this study is a qualitative and functional thesis. Literature review and participant observation are used to collect data, and content analysis is used to analyse the collected data. The strategy and the methods are explained in more detail in this chapter.

3.1 Qualitative and Functional Thesis

The purpose of qualitative research is to understand a phenomenon without using statistical or other quantitative methods. Unlike quantitative research, it does not attempt to make generalisations and it is not based on a specific theory or well-known models. Instead, the goal is to have a thorough view on the subject under research, and the results are only applicable to the specific case. The phenomenon is described using the written word rather than through figures, and thus, qualitative research is descriptive in nature. The logic is typically inductive, that is to say, reasoning progresses from individual instances to conclusions. (Kananen 2014a, 16-20.)

Different techniques for qualitative research are, for example, case research, action research, functional research, and ethnographic research. The combination of qualitative and quantitative strategy is blended research. A variety of methods can be used to collect and analyse data. A qualitative research process in cyclical in nature. Analysis is part of every phase of research, from the gathering of material to final conclusions, and it guides and supports the entire process. There is a direct link between the researcher and the phenomenon under research. The research is carried out in the genuine context of the phenomenon: the researcher enters the field to do interviews or to make observations, for example. (Kananen 2014a, 18-22.)

A functional thesis combines theory and actions, and it is an alternative to a thesis that is more focused on research. Despite this, it must fulfil the general requirements of an academic thesis by including, for example, an adequate level of research communication. A functional thesis is by nature heavily grounded in practical work. The purpose is to produce something concrete: instructions, guidelines, a programme, or an event, for example. Theory is applied to find a suitable approach and a basis for decisions. The theoretical framework and definitions guide the thesis process. (Vilkka & Airaksinen 2003, 5-50.)

A functional thesis must always explain the entire creation process of the final product. The execution of the product should be such that it benefits the target group as much as possible. Things to consider when planning a product are usability, costs, image, and scale, among other things. The final thesis report is a description and evaluation of the process, results, and conclusions. It is written alongside the development of the resulting product. Both of these processes, writing and development, complement each other and should be inseparable. (Vilkka & Airaksinen 2003, 51-67.)

3.2 Methods

A literature review is the first method of collecting data for this thesis. Chapter four is based on this method. By doing a literature review, a researcher proves that they are aware and are able to interpret what is already known about the phenomenon. A literature review has many benefits. It deepens the understanding of the study field before the actual research process begins. However, the researcher must be aware of the possible problem this poses: fixed perceptions of the phenomenon may narrow down the perspective and affect, consciously or unconsciously, decisions made during the research. A literature review helps in defining terminology and in finding the right meters, among other things. By doing this, the researcher can ground the study to existing theory. The use of literature also increases the validity of research because existing material supports the researcher in making decisions and conclusions. (Kananen 2009, 74-76; Jesson, Matheson & Lacey 2012, 10.)

Before a literature review can be carried out, a research question must be defined. The research question will then determine the focus and scope of the literature review. (Jesson et al. 2012, 18-19.) According to Kananen (2009, 73), written sources include materials gathered through observing, interviews, and a research diary during the thesis process, as well as existing documents connected to the phenomenon. In this thesis, the literature used is published works and websites in the field of risk and research methodology, and unpublished company-specific documents.

The second method of collecting data for this thesis is participant observation. The method of observation is used to get information about people's actions and behaviour. It takes into account both verbal and nonverbal expression. It is a method where the researcher participates in the activities of the research subjects and in this way, becomes a member of their group, organisation, or community. Consequently, the researcher does not just observe the phenomenon, but also feels it. (Gill & Johnson 2002, according to Saunders, Lewis & Thornhill 2009, 289-290; Havainnointi eli observointi 2015.) This involves an immersion in the research setting (Delbridge & Kirkpatrick 1994, according to Saunders, Lewis & Thornhill 2009, 290).

A participant observer can have different roles. Gill and Johnson (2002, according to Saunders, Lewis & Thornhill 2009, 293-294) have identified the following four roles: complete participant, complete observer, observant as participant, and participant as observer. A complete participant and a complete observer do not reveal their researcher identity. The researcher's position in this study resembles the most the role of an observer as participant. An observer as participant does not participate in the activities in the same way as main participants, but rather focuses on observing and assisting. (Gill & Johnson 2002, according to Saunders, Lewis & Thornhill 2009, 293-294.) The observations will be made in the workshops as well as throughout the process through different methods of communications, such as face-to-face discussions and emails. An observational checklist is presented in Appendix 1. Additionally, other observations made throughout the process will be taken into account.

Content analysis is used to analyse the collected data. According to Tuomi and Sarajärvi (2018, 103), content analysis is a basic analysis method in qualitative research, and most of the methods in qualitative research are actually based on content analysis. Its purpose is to produce concise and clear content of the research material which will then help the researcher to make reliable conclusions. The material can be anything in written form, such as transcribed interviews, articles, report, and memos. (Ojasalo, Moilanen & Ritalahti 2009, 121.)

Content analysis is based on logical deduction and interpretations. The main phases are the collecting and preparing of the research material, the simplification of the research material, and recognition and interpretation of recurrent patterns. Critical review is part of all these three phases. Before the analysis can begin, the researcher must decide if they are only going to analyse the manifest content or also the latent content. In this thesis, content analysis is used to go through the manifest content of the local risk assessment results. (Ojasalo, Moilanen & Ritalahti 2009, 121-123.)

Validity and reliability are concepts that are used to assess the results of a research. Validity refers to how well the methods and findings represent the phenomenon the researcher is studying. Reliability refers to consistency: if the research was to be repeated, the results should remain the same. Validity is focused on research design and partly on the analysis of data. Reliability is connected to the execution of the research. (Kananen 2014a, 146-147.) A functional thesis must abide by certain ethical rules. The goals should be morally sound, the development project is to be conducted with honesty and care, and the results must be truly applicable in practice. (Ojasalo et al 2009, 48-50.)

4 Risk Management

Risk management is an essential component of a business' strategic management. It is to be a continuous, developing process which considers risks related to past, present, and future activities. Systematic and clearly communicated risk management can increase the level of trust and respect towards the company. (A Risk Management Standard 2002, 2; Leino, Steiner & Wahlroos 2005, 145). This chapter first describes security and then the nature of risk, especially from an organisational point of view. Some examples of categorising risks are given. Then, the concepts of corporate governance and enterprise risk management are explained. The risk management process is introduced by presenting some of the most common approaches. The focus of this thesis, risk assessment is described in more detail.

4.1 Security

The concept of security refers to an objective and external state, or a subjective and experienced state, or a relationship between the former and the latter. First of all, security can be seen as a basic human need, and the fulfilment of needs is the basis of well-being. (Maslow 1987, Alderfer 1972, Riihinen 1979 according to Niemelä 2000, 21-22.) Secondly, security is a humane and social value. It is predictability, tranquillity, and the absence of dangers (Kaufmann according to Niemelä 2000, 22). Thirdly, security can be considered a basic human right. People have their own impressions of security which are based on experiences, observations, and what they have learned. The feeling of security comes from routines, stability, trust, and predictability. Security and insecurity are part of all areas of human life. Security is defined in different ways depending on the context. For example, information security can be defined as the protection of sensitive information. The concepts of risk, threat, danger, and fear are closely related to insecurity, the opposite of security. Risk assessments are connected to the feeling of insecurity and the attempt to manage this feeling. Risk management aims to reduce existing insecurity and to make the future as secure as possible. (Niemelä 2000, 23-25; Purpura 2011, 9 & 324; Tikkanen et al. 2009, 13.)

When it comes to organisations, security can be defined as a state where there are no uncontrollable, unpredictable, or sudden events that result in losses. Risks are on an acceptable level and their mitigation is efficient. The role of security in an organisation is the protection of employees, assets, operations, environment, and reputation. The goal is to ensure that the set objectives are reached without interruptions. This is achieved by methodology and strategies. The security methodology serves as the foundation for the implementation of security strategies. It includes methods, disciplines, theories, and concepts, for example. Security strategies, derived from the methodology, refer to the application of different aspects of security, such as physical security and information security. Different strategies are deterrence, deception, detection, delay, denial, mitigation, and response. These strategies protect, for example, from violence, theft, computer crime, fire, accidents, fraud, espionage, substance abuse, disasters, and terrorism. Risk management is the foundation of corporate security, because decisions connected to security should be based on a risk analysis. (Purpura 2011, 10-11; Tikkanen et al. 2009, 13 & 88-104.)

The security risk assessment of the case company is heavily focused on information security. The fundamental principles of information security are confidentiality, integrity, and availability. This is often referred to as the CIA triad. The goal of confidentiality is to ensure the appropriate level of secrecy and to prevent unauthorised disclosure. Integrity is concerned with the accuracy and reliability of information and the prevention of unauthorised modifications. The purpose of availability is to guarantee that authorised users have timely access to data and resources. Controls to minimise information security risks can be administrative, technical, and physical, for example, training, firewalls, and locked server rooms. These are categories of controls. When a variety of controls are used, this is called defense-in-depth. Different functionalities of information security controls are preventive, detective, corrective, deterrent, recovery, and compensating. (Harris & Maymi 2016, 3-10.)

4.2 Organisational Risks

Risks that are related to organisations can arise from a variety of sources. Merna & Al-Thani (2010, 16) provide a list of typical sources: political, environmental, planning, market, economic, financial, natural, project, technical, regulatory, human, criminal, safety, and legal. In short, a risk source can be anything that can have an influence on business. If this influence is uncertain and significant, it gives rise to a risk. (Merna & Al-Thani 2010, 16-17.)

There are many ways to classify risks. Risks can be either dynamic or static. Dynamic risks, such as political and financial risks, are affected by situational factors, and they can have both positive and negative outcomes. Business risks are usually dynamic in nature. Static risks, on the other hand, have only negative outcomes. They are easier to predict than dynamic risks. Static risks are pure and insurable risks which are not significantly affected by the business environment. (Kuusela & Ollikainen 2005, 31-34.)

Hopkin (2017, 17) uses the following model of four categories: compliance or mandatory risks, hazard or pure risks, control or uncertainty risks, and opportunity or speculative risks. Compliance risks are minimised, hazard risks mitigated, control risks managed, and opportunity risks embraced. An opportunity risk is an example of a risk that can have a positive outcome. (Hopkin 2017, 17.)

Moeller (2007, 25) presents a sample of what an organisation’s risk model could look like. It has four categories: strategic risks, operations risks, finance risks, and information risks. Strategic risks include external factor risks, such as economy risks, and internal factor risks, such as reputation risks. Operations risks comprise of process, compliance, and people risks. Treasury, credit, and trading risks are all finance risks. Information risks refer to financial, operational, and technological risks. (Moeller 2007, 25.)

4.3 Corporate Governance and Enterprise Risk Management

The terms “corporate governance” and “risk management” often appear in the same context. The Organization for Economic Cooperation and Development, OECD (G20/OECD Principles of Corporate Governance 2015, 9) sees corporate governance as a set of relationships between management, the board, shareholders, and other stakeholders. It is a structure that helps an organisation to define its objectives, to find the means to achieve them, and to decide how performance is monitored. Corporate governance is a combination of processes and organisational structures which the management has created. The goal is to have a corporate environment which is characterised by trust, transparency, and accountability. This environment is a basis for long-term investments, financial stability, and business integrity, which in turn support growth. The OECD has published principles of corporate governance to guide organisations with their governance practices. (G20/OECD Principles of Corporate Governance 2015, 7-9; Hyvä hallinto- ja johtamistapa (corporate governance) 2017.)

Leino et al. (2005, 124) state that corporate governance is a mechanism for managing and controlling a business. In other words, it describes how an organisation is managed. An important element of corporate governance is internal controls. Their purpose is to ensure that objectives are reached, resources are used wisely, and risks are efficiently managed. Thus, risk management is part of internal controls and corporate governance. Consequently, management is responsible for suitable risk management. This can be seen in corporate governance recommendations. (Leino et al. 2005, 123-126.) In Finland, for example, a listed company should first set forth the principles for internal auditing, and then describe how its risk management is organised. Shareholders are to be informed of significant risks. (Suositus listayhtiöiden hallinnointi- ja ohjausjärjestelmistä (Corporate Governance) 2003, 13.)

Hopkin (2017, 4) summarises the reasons for risk management as mandatory, assurance, decision-making, and effective and efficient core processes. The ultimate goal is to bring value. (Hopkin 2017, 4-56.) There are several external and internal requirements which direct organisations in risk management. External requirements come mainly from legislation, risk management standards, recommendations specific to a business field, and customer contracts. Internal requirements are those that have been agreed upon through the company vision, values, strategies, policies, and guidelines, for example. In addition to requirements, the increasingly rapid change in environments, particularly due to globalisation and digitalisation, make risk management an essential part of a successful business. (Ilmonen, Kallio, Koskinen & Rajamäki 2013, 18-19; Merna & Al-Thani 2010, 1.)

Enterprise Risk Management (ERM) is a holistic approach to managing risks that is commonly used in large organisations. According to ERM, risk management is a multidirectional and continual process where all different areas are interrelated. (Hopkin 2017, 96; Ilmonen et al. 2013, 26.) The basic idea behind ERM is that the goal for all business units is to create value for stakeholders. The benefits of ERM are considered to be better management of uncertainties, minimisation of losses, achievement of targets, and maintaining reputation. For ERM to be successful, it must be tied to a company’s strategic and planning processes, daily monitoring and reporting, and internal auditing, for example. (Leino et al. 2005, 126-136.) An example of an ERM framework is COSO ERM, published in 2004, which is designed for organisations of all sizes and types (Moeller 2007, x). It has four main objectives: high-level goals which support the company mission, efficient use of resources, reliable reporting, and compliance with laws and regulations (Enterprise Risk Management – Integrated Framework. Executive Summary 2004, 3).

4.4 Risk Management Process

According to Merna and Al-Thani (2010, 2), risk management is a formal process which includes four main phases: identification, assessment, planning, and management of risks. All levels of an organisation should participate in this process. Risk management involves coordinated activities, the goal of which is to direct and control organisations in relation to risks. It creates and protects value. It supports organisations with their performance, innovation work, and achievement of goals. The principles of good risk management, as seen in the ISO 31000 standard, are illustrated in Figure 2. Risk management should be integrated, structured and comprehensive, customized, inclusive, and dynamic, use the best available information, take human and cultural factors into account, and be continually improved. (ISO 31000:2018, 6-8).

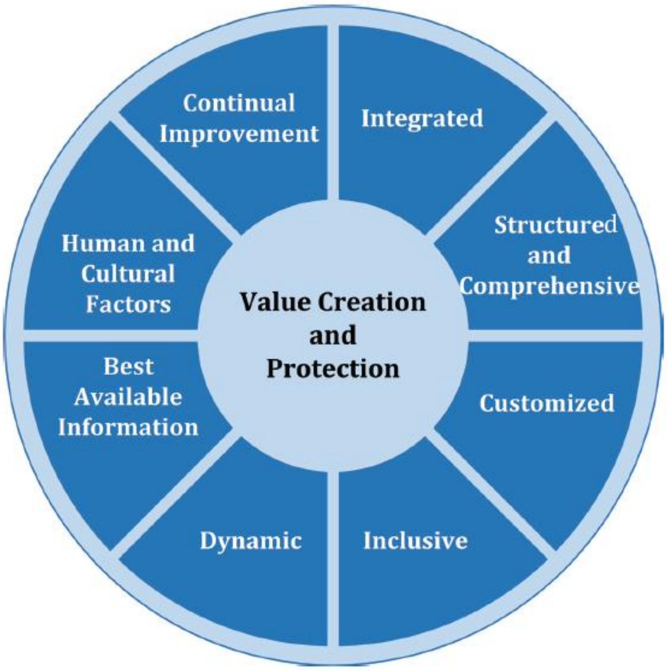

Continual Improvement
Integrated
Human and Cultural Factors
Structured and Comprehensive
Value Creation and Protection
Best Available Information
Customized
Dynamic
Inclusive

Figure 2: Principles of good risk management (ISO 31000:2018, 8)

An organisation's risk management process is typically based on a standard. According to Hopkin (2017, 72), a risk management standard describes a risk management process and a recommended framework. The most common standards are ISO 31000, IRM Standard, and the COSO ERM. (SFS-ISO 31000:2018; A Risk Management Standard 2002; Enterprise Risk Management – Integrated Framework. Executive Summary 2004.) All the standards follow more or less the same basic structure: 1) setting of a risk management scope, 2) identifying threats and opportunities, 3) assessing risks, 4) planning and implementing risk management responses, 5) reporting and communicating, and 6) evaluating the quality and success of risk management regularly (Ilmonen et al. 2013, 27).

ISO 31000 (2018, 9) provides an example of risk management framework as illustrated in Figure 3. This sees risk management as a continuous process which is made up of integration, design, implementation, evaluation, and improvement. An essential part of this framework is the support of leadership and commitment. (ISO 31000:2018, 9.)

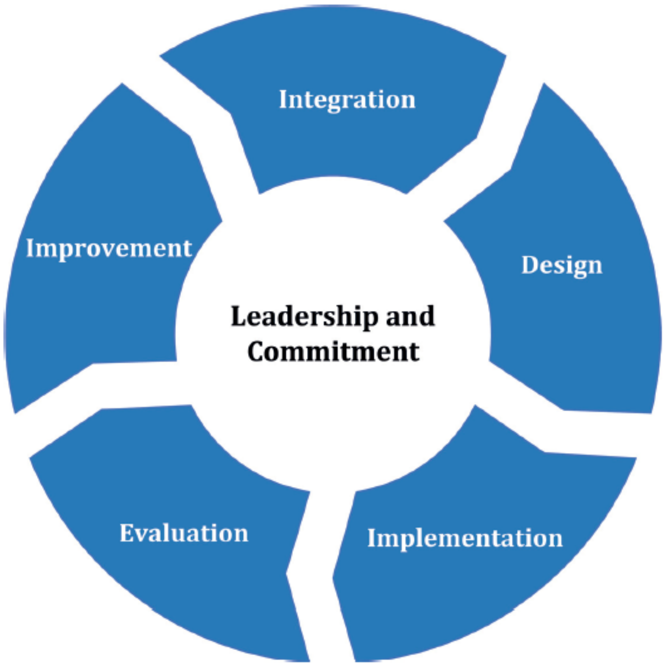


Figure 3: Risk management framework (ISO 31000:2018, 9)

Figure 4 is based on the ISO 31000 standard, and it presents a typical risk management process. It begins with establishing the scope, the context, and the criteria. The next phase, on which this thesis focuses, is the risk assessment phase which includes risk identification, risk analysis, and risk evaluation. This is followed by risk treatment which includes selecting and implementing appropriate ways to address risks. The whole process is supported with communication, consultation, monitoring, and review. (ISO 31000:2018, 13-19.)

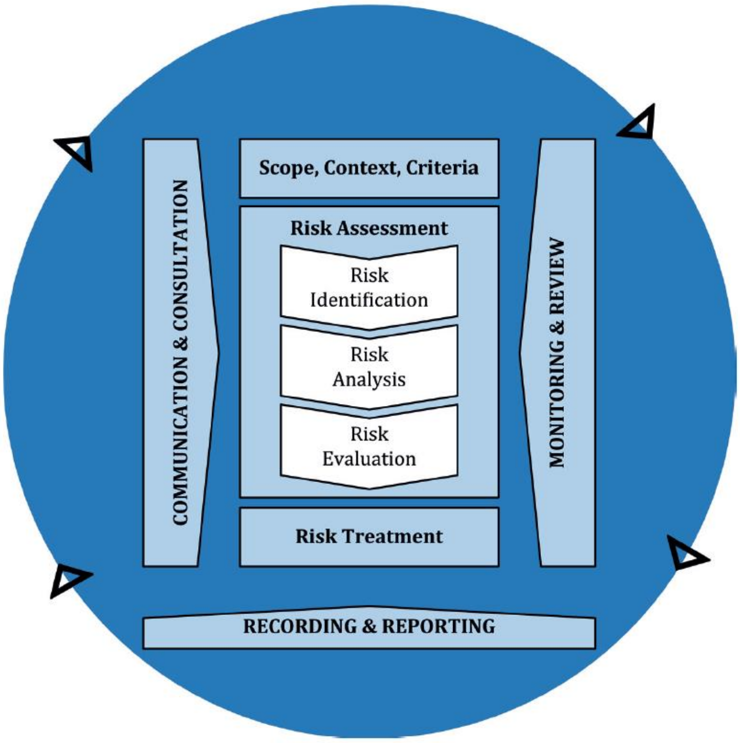


Figure 4: Risk management process (ISO 31000:2018, 16)

The very first step is to establish a scope and to make sure that it is clearly communicated to all relevant parties. The process can be applied to a strategical level or it may only concern an individual project, for example. When establishing a scope, the following points should be considered: objectives, expected outcomes, time, location, inclusions and exclusions, tools and techniques, resources, responsibilities, records, and relationships with other processes and activities. (SFS-ISO 31000:2018, 14.)

Both internal and external context that have the potential to affect the achievement of an organisation's objectives are to be established. This is a crucial step that has an effect on the subsequent risk assessment. External context can be divided into three categories: 1) international, national, regional and local social, cultural, political, legal, regulatory, financial, technological, natural, and competitive environments, 2) key risk sources and trends associated with the organisation, and 3) external stakeholders. The internal context includes organisational structure and culture, roles, responsibilities, capacity, capabilities, internal systems, and internal stakeholders. The established context is documented in written form, approved by management, and used for monitoring and review. (ISO 31000 Risk Management. A practical guide for SMEs 2015, 39-42.)

The criteria states organisational objectives, values, resources, and legal and regulatory obligations, and it is to be in line with the organisation's policies. The criteria should include:

1) the nature and type of causes and consequences and how they are measured, 2) how likelihood is defined, 3) the timeframe for likelihood and consequences, 4) how risk levels are calculated, 5) stakeholder views, 6) the level of acceptable risks, and 7) how the combination of risks is considered. The criteria helps to determine the significance of risks and to compare risk levels. (ISO 31000 Risk Management. A practical guide for SMEs 2015, 47-49.)

4.5 Risk Assessment

Risk assessment has several objectives. It is a process that helps organisations to make decisions to control and manage risks in a cost-effective and efficient way. It provides a method for examining threats, vulnerabilities, and their impact. Risk assessment brings risk awareness among employees and guides them in contributing to risk control. It is a basis of successful risk management and it helps to ensure that risk management meets business objectives. (Burns-Howell et al. 2003, 17.) Risk assessment typically includes three phases: risk identification, risk analysis, and risk evaluation. It should be an exercise which is conducted regularly and which involves several stakeholders who all bring their respective expertise and views to the table. (ISO 31000:2018, 15.)

In risk identification, relevant risks are identified and described. Relevant risks are those that have some level of probability of affecting a business within a time period that is considered reasonable. An efficient approach is to involve employees at all levels of the organisation, who will help identify and assess risks in their own units. The COSO ERM models proposes a brainstorming approach to start off the identification phase. (Moeller 2007, 23-24.)

Risk identification is a critical task because only those risks that have been identified will be considered in the following phases of the risk management process. Risk identification should include both internal and external risks. The review of external and internal context, established in the previous stage, helps to identify these risks. It is crucial to have up-to-date information for the results to be valid and reliable. Once the risks have been identified, sufficient information should be provided for each risk. This includes objectives that could be impacted, the context of the risk, conditions or sources that are required for the risk to materialise, possible consequences of the risk, and current controls for the risk. (ISO 31000:2018, 15-16; Merna & Al-Thani 2010, 47; ISO 31000 Risk Management. A practical guide for SMEs 2015, 63-64.)

Identified risks are typically presented in the form of a risk register. At the same time, a risk register can be used to record current controls and to recommend future controls to better manage risks. A possible downside of this practice is that only threats in the register are considered and the risk management process is no longer sufficiently dynamic. A risk register should rather be viewed as an action plan which describes the current status of the risk management and the needed controls. (Hopkin 2017, 88-92.)

The second step is to analyse the identified risks and to determine risk levels. In this phase, an understanding of risks is developed. The factors considered here are typically uncertainties, risk sources, consequences, likelihood, events, scenarios, and controls and their effectiveness. The approach can be qualitative, quantitative, or both. Usually the approach and methodology is determined by the risk management framework. (ISO 31000:2018, 16-17; ISO 31000 Risk Management. A practical guide for SMEs 2015, 65-66.)

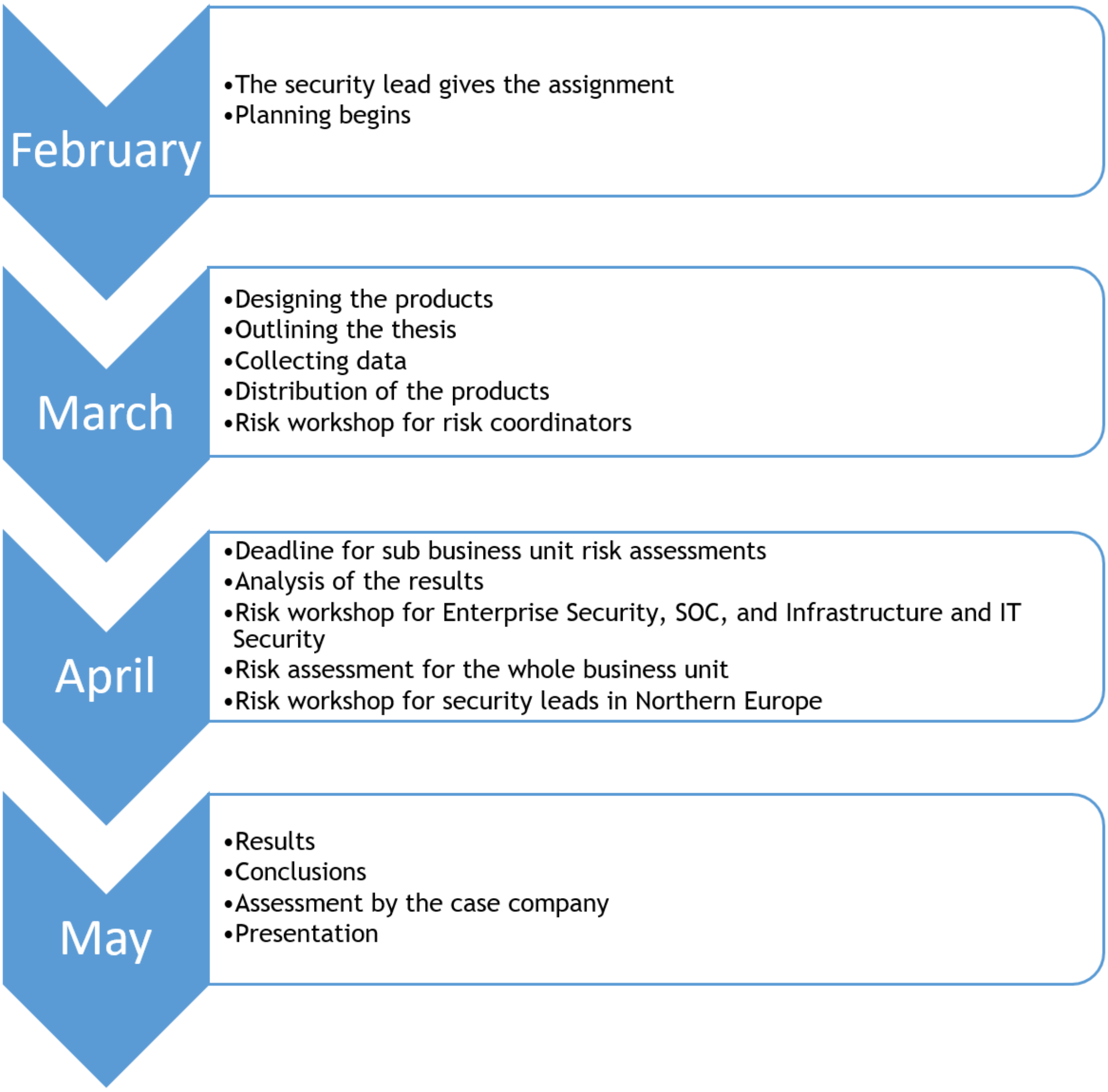
Some of the qualitative techniques for analysing risks, according to Merna and Al-Thani (2010, 68-76), are brainstorming, assumption analysis, Delphi, interviews, hazard and operability studies (HAZOP), failure modes and effects criticality analysis (FMECA), checklists, prompt lists, risk registers, risk mapping, probability-impact tables, risk matrix charts, and project risk management road mapping. Quantitative techniques include decision trees, a control interval and memory technique, a Monte Carlo simulation, a sensitivity analysis, and a probability-impact grid analysis. The technique used in the case company’s risk assessment is probability-impact tables, which represent a qualitative approach. Assessing risks is not based on an exact science, but rather on subjective estimations. The same circumstances can yield different results when different individuals assess risks. Because perceptions, opinions, and judgements can have an impact on the results, it is important to involve several stakeholders in this process. (Merna & Al-Thani 2010, 33-84.)

The final step of risk assessment is risk evaluation. Its aim is to support decisions made about risk treatment. Risk analysis results are compared with the company’s risk appetite, and based on this, risks are either accepted or treated. (ISO 31000:2018, 17; ISO 31000 Risk Management. A practical guide for SMEs 2015, 66.) If in risk evaluation, the last phase of risk assessment, there are intolerable risks that are not sufficiently controlled, risk treatment is called for. Risk treatment methods should be cost-efficient and in line with external requirements. Different risk treatment options are: 1) avoidance, 2) pursuance of opportunities, 3) changing the likelihood, 4) changing the consequences, 5) sharing the risk, and 6) retaining the risk. The goal of risk treatment is to reduce the risks that have potentially negative effects and increase the risks that have potentially positive effects. (ISO 31000 Risk Management. A practical guide for SMEs 2015, 67-69.)

Both the risk management framework and the process should be regularly monitored and reviewed. The ISO 31000 standard recommends the method of Plan-Do-Check-Act for this purpose. (ISO 31000 Risk Management. A practical guide for SMEs 2015, 73.) Monitoring helps to assure that the right controls are deployed and the agreed procedures are followed. If there are significant changes in the business environment, required modifications must be made accordingly. (A Risk Management Standard 2002, 11.) The purpose of communication is to improve awareness and understanding of risks. Consultation, on the other hand, provides feedback and support for the risk management process. Communication and consultation should involve all relevant stakeholders and be part of every phase of the risk management process. Finally, the whole process and the results have to be documented. The purpose of recording and reporting is to inform the whole organisation about the risk management and its results, to provide relevant information that aids decision-making, to improve risk management, and to support interaction with stakeholders. (ISO 31000:2018, 14-19.)

5 Process

This chapter describes the whole process of this functional thesis. The aim is to validate the study: if the same steps are repeated, the result should remain the same. The process has been divided into the following phases: planning and preparing, and execution and finalising. The process flow in the spring of 2018 is presented in Figure 5.



February

- The security lead gives the assignment
- Planning begins

March

- Designing the products
- Outlining the thesis
- Collecting data
- Distribution of the products
- Risk workshop for risk coordinators

April

- Deadline for sub business unit risk assessments
- Analysis of the results
- Risk workshop for Enterprise Security, SOC, and Infrastructure and IT Security
- Risk assessment for the whole business unit
- Risk workshop for security leads in Northern Europe

May

- Results
- Conclusions
- Assessment by the case company
- Presentation

Figure 5: The process flow

5.1 Planning and Preparing

The actual development process began before it became thesis work when in February 2018 Finland's security lead introduced the problem he had identified. After some planning on how to conduct risk assessment in the sub-business units, it became clear that the amount of work in the project is rather extensive. Thus, near the end of February the project was turned into a functional thesis and thesis planning could begin.

The first stage was to outline an initial structure for the thesis and to collect data for the theoretical framework. This took place in March. Due to a fairly tight schedule, the new risk assessment tool and supporting material was continuously developed alongside this. The development of the tool began with designing a clear and practical layout. Only after this were the formulas and functions added. The supporting material was written using internal company material and electronic references that were considered reliable. Finland's security lead gave feedback during this development phase. For example, he suggested making the tool look more like other Excel documents used in the company by removing additional information from the main sheet. He wished to have two additional tables for possible new risks and comments below the four security risk domains.

During the designing phase, the scope of security risks changed, and the products had to be modified accordingly. Two risk domains were excluded from security risks and moved to another risk area. The two tables were removed from the tool and the functions changed accordingly. This also meant that some of the threats had to be taken out of the supporting material and the numbering of risks was changed. Once the tool and the other material were finished, an invitation was sent to sub-business units' risk coordinators to take part in a security risk assessment kick-off workshop. This was organised by Finland's security lead and the author of this thesis at the end of March.

In the kick-off workshop in March, the risk assessment process was first explained to the risk coordinators. After this, the new risk assessment tool was introduced by presenting the idea behind it and by showing how it should be filled in. The sub-business units were given a deadline by which their risk assessment must be finished and be sent to the writer of this thesis to be further processed. This gave them two weeks to complete the task. To support the risk assessment, the risk coordinators were given the opportunity to have individual workshops with the author of this paper.

During the risk assessment period, some questions arose which needed clarification, and this gave ideas to develop the supporting material further. For example, it was suggested by one risk coordinator that the impact and velocity should always be the same when critical or sensitive information is lost, regardless of the source of threat. It was clarified by the writer of this thesis that the nature of the threat does indeed affect impact and velocity. As an example, the impact is likely to be smaller if an employee loses a laptop than if the entire company network is hacked. Laptops are locked and encrypted, and they can be remotely wiped. The impact would be very limited and the incident solved quickly. An entire network would have larger amounts of critical and sensitive information. It would be more difficult and laborious to remedy the incident, and the impact would be much greater as this incident would affect a large number of employees. This could also result in bad publicity and potentially in losing customers.

No individual risk workshops were requested. Most of the risk assessments were returned by the given deadline in early April. Three risk assessments were not returned on time. Reminders were sent to those who had not delivered theirs. In the end, altogether eight risk assessments were completed. One assessment for a fairly large sub-business unit was not returned at all.

5.2 Execution and Finalising

After receiving the risk assessment results for most of the sub-business units, they were brought together in one document which would later be used in the next workshop in April 2018. The results included the assessment of predefined risks, assessment of new identified risks, and other comments. Next, a business unit level workshop was arranged between global security, including Finland’s security lead and the writer of this thesis, the Security Operation Centre (SOC), and the Infrastructure and IT Security department. The idea of this workshop was to go through the findings and to make a risk assessment of the whole business unit.

Initially, the plan was to use the original, enterprise-level tool in this workshop, but it was decided to take advantage of the newly-developed tool because it was considered suitable for a risk assessment workshop. This business unit level risk assessment was not based on the averages of sub-business units’ assessments, because sub-business units vary in size, nature, and significance, and the final assessment is made by the security lead. Instead, the results were to be used as reference and support for making an accurate risk assessment for the whole business unit of Finland and Estonia.

After the business unit level workshop in April, Finland’s security lead and the writer of this thesis transferred the results to the original enterprise-level tool. At this stage, all the decisions made in the business unit level workshop were considered one more time, and the sub-business unit risk assessments were reviewed again. As a result, some changes were still made in order for the risk assessment to be as accurate and realistic as possible. For example, it was decided that in the previous workshop, some of the values for threats had been estimated too high, and they were slightly lowered. Also, all the other risks identified in the sub-business units were discussed. It was concluded that some of those risks, for example business continuity, were already included in other risk areas. Some risks could be considered to be part of the existing security risks. For example, the threat of incorrectly understanding a situation and not reporting it properly, could be categorised as human error.

After filling in the data in the enterprise-level tool with the final values for threat, vulnerability, and impact, the justifications for all the decisions were written down in the provided section. The risk level for one security risk domain, Protecting sensitive and critical information, became high. This risk domain includes the following threats: equipment, media, and documents theft or loss, human error, hacking, system sabotage, system intrusion, insider threat, malware, sniffing or tampering communications, and social engineering attacks. These are threats that large companies in particular face regularly. These threats also develop quickly. For example, new malware variants are constantly being authored. This means that companies have to be able think on their feet and improve and modify their controls quickly. Actions are required to mitigate and control risks that have a high risk level. For this particular domain, a root cause description of significant threats and control weaknesses, and a potential business impact were provided. This will help the planning of risk treatment. Other risk domain levels were either moderate, low, or very low. Moderate risk levels are monitored, low and very low risk levels are accepted. (Internal material about risk management 2018.)

The thesis process culminated in a strategic business unit level risk workshop in April 2018 where Finland’s security lead and the writer of this thesis presented the risk assessment results and the newly developed tool for other business units in Northern Europe. The current status of the company risk management was discussed and areas of improvement were found. These included the lack of cooperation and resources. Finally, the results were analysed and documented in this thesis in May 2018.

6 Results

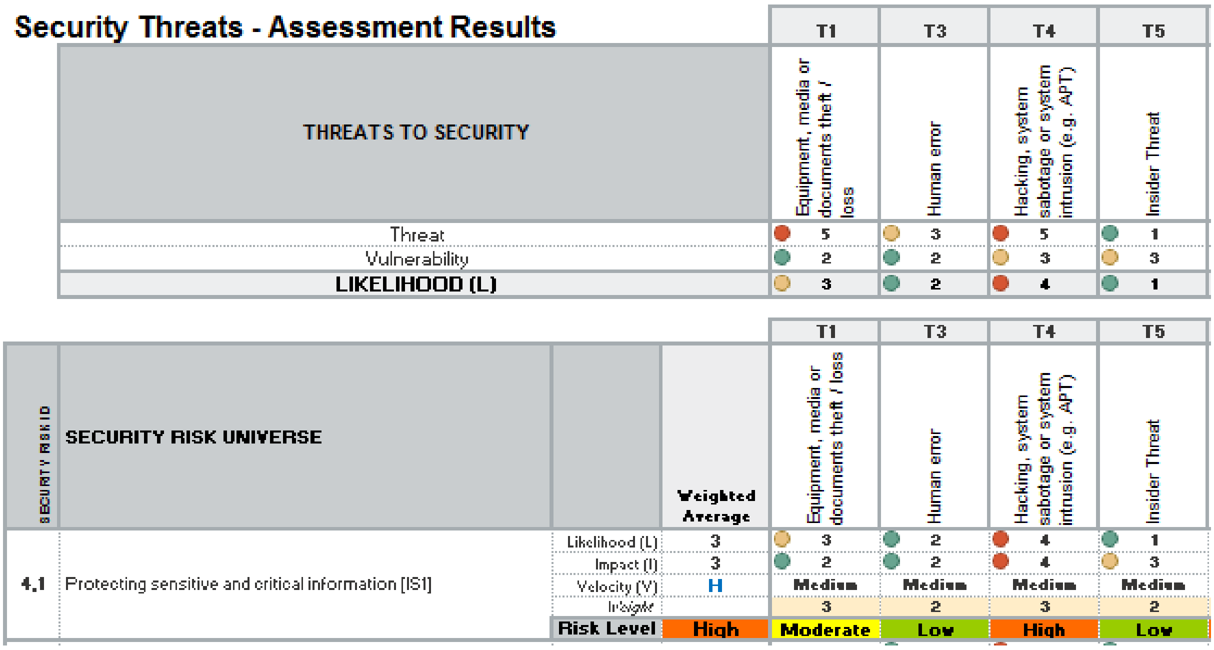
The concrete outcome of this research is a local risk assessment tool which is used to provide accurate results for the enterprise-level risk assessment tool. In addition, supporting material was compiled to help the risk assessment process in workshops. The development of the tool and the supporting material are presented in this chapter. The final products are the case company’s intellectual property and for this reason will not be presented in this thesis in their entirety. The results of participant observation and the responses of relevant stakeholders are included in this chapter.

6.1 Products

The company has an enterprise-level risk assessment tool. It is a complicated, Microsoft Excel-based tool which is best suited for reporting the final results for the entire business unit. Finland’s security lead recognised a need for a more simple and straightforward way to assess risks in sub-business units. Thus, the original tool was converted into a more suitable tool which was first introduced in workshops for the relevant sub-business unit representatives and then for security leads of other business units.

The main criterion for the new tool was that it should easy to comprehend and to use, even if the user is not experienced in assessing risks. It must be highly automated in terms of calculations, and it should eliminate the possibility of erroneous use as far as possible. The results are to be clearly visible with the help of a straightforward layout, colours, and summarising tables.

The enterprise-level tool comprises user guidelines, general information, scope, risk analysis, results, and scales. The actual risk assessment is done in the risk analysis section. It is a very intricate tool, and in addition to the cells in which values are given, it contains information and space for explanations. As mentioned previously, this is more suitable for the final results and not for a hands-on workshop. The results of the risk assessment appear in the results section as shown in Table 2. This is only a small sample of the multi-sheet tool.



Security Threats - Assessment Results

THREATS TO SECURITY	T1	T3	T4	T5
	Equipment, media or documents theft / loss	Human error	Hacking, system sabotage or system intrusion (e.g. APT)	Insider Threat
Threat	🔴 5	🟡 3	🔴 5	🟢 1
Vulnerability	🟢 2	🟢 2	🟡 3	🟡 3
LIKELIHOOD (L)	🟡 3	🟢 2	🔴 4	🟢 1

SECURITY RISK ID	SECURITY RISK UNIVERSE		Weighted Average	T1	T3	T4	T5
				Equipment, media or documents theft / loss	Human error	Hacking, system sabotage or system intrusion (e.g. APT)	Insider Threat
4.1	Protecting sensitive and critical information [IS1]	Likelihood (L)	3	🟡 3	🟢 2	🔴 4	🟢 1
		Impact (I)	3	🟢 2	🟢 2	🔴 4	🟡 3
		Velocity (V)	H	Medium	Medium	Medium	Medium
		Weight		3	2	3	2
		Risk Level	High	Moderate	Low	High	Low

Table 2: Risk analysis results in the Enterprise Security Risk Assessment tool

Table 2 shows security risk domain 4.1: Protecting sensitive and critical information. This means that a company's and clients' information must be protected from being leaked or disclosed without authorisation. This information includes personally identifiable information. T1, T3, T4, and T5 are threats to sensitive and critical information. Threats have first been identified and only then categorised, and consequently T2 does not apply to 4.1. The identified threats can be reduced with process, people, and IT controls. Different controls for T1: equipment, media or documents theft or loss, include policies, disk encryption, and authentication. The risk of T3: human error, can be reduced with insurances, backups, and training. Security monitoring and firewalls are used to control T4: hacking, system sabotage or system intrusion. Controls for T5: insider threat, include sanctions, separation of duties, and contractual agreements. These are only some examples of possible controls. Other threats to protecting sensitive and critical information are malware, sniffing or tampering communications, and social engineering attacks. The tool presents all of the four security risks and threats related to them in the same manner.

Unless the reader is familiar with the layout, it is somewhat difficult to read and to interpret the results. The structure of the table is two-fold, and the text is both vertical and horizontal. Apart from risk levels, the depictive colours are only small circles instead of filling the entire cell. In the new version, the different threats under a risk domain have been presented on the left side of the chart (Appendix 2). Every risk domain has its own chart, and the weighted averages of that particular risk domain are calculated automatically in the small table under the main table.

The workshop tool takes advantage of several formulas and functions. Designing and implementing these has been the most time-consuming part of the development process. The workshop participants are presented with a table which contains only the names of threats and their weight. First, the participants are instructed to fill in a value between 1 and 5 for threat and vulnerability. They can either type in the number or use the drop-down list. A value outside the range will prompt an error message. All the colours in the tool are inserted automatically based on the values. After the values for threat and vulnerability have been filled, the likelihood is calculated automatically.

Next, impact is given a value between 1 and 5. Velocity can be either low, medium, or high. Also these values can be either written or chosen from the drop-down list. The velocity column uses a function which assigns a numerical value for each option: 1 for low, 2 for medium, and 3 for high. As a result, it is possible to calculate the weighted average for velocity. Weight is based on predetermined values, and it is used in the weighted average calculations.

The risk level is calculated automatically based on the values in the columns for likelihood and impact. The risk level column uses a function which turns a numerical value into a word: very low for 1, low for 2, moderate for 3, high for 4, very high for 5. The resulting risk level is clearly indicated with a colour and a word. The smaller, weighted average table uses formulas to automatically calculate the results for the particular risk domain based on the main table. The weighted results from these tables are automatically transferred to a table that summarises the result (Appendix 2). This table is presented at the top of the tool so that the reader can quickly get an idea of all the risks in the sub-business unit.

Those who participate in the risk assessment workshops do not necessarily have in-depth knowledge or experience of the threats that are to be assessed. The participants are all appointed as risk coordinators for their sub-business unit, but some of them are fairly new in their role and have only assessed current risks instead of risks for the entire coming fiscal year. Some of the threats, for example advanced persistent threat (APT), are very specific to IT, and the risk coordinators do not necessarily have a technical background. For these reasons, it was considered useful to create an informative Security Risk Guide.

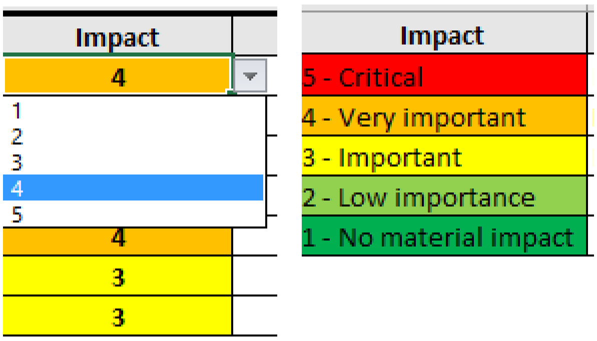
The Security Risk Guide took the form of a PowerPoint presentation. It was created in Finnish because it was suspected that some of the possible difficulties in assessing risks could be due to the English terminology. First, the guide introduces the four risk domains and lists all the threats related to them. For example, the risk domain of Safeguarding physical assets and facilities includes the following threats: criminal or interpersonal threats and violence, physical threats and hazards, and natural disasters. Then the guide gives very concise explanations for the threats identified in the risk assessment tool and lists protective measures. For example, natural disasters include storms, earthquakes, floods, and wildfires. Protective measures are, for example, an uninterruptible power supply (UPS), business continuity plans, and crisis management. Also, supporting questions for the risk assessment work are provided. For the risk domain of Safeguarding physical assets and facilities it is: “What are the most critical assets?” The threats covered in the presentation are the same as in the risk assessment tool. It was considered best to keep the guide as short as possible so that the busy risk coordinators would use it for support. The PowerPoint presentation includes eleven slides of bulleted lists. An excerpt of the guide is provided in Appendix 3.

6.2 Observations and Response

The security leads, risk coordinators, and other relevant stakeholders were observed throughout the thesis process in risk workshops and through other means of communication. Unfortunately, the opportunities for systematic participant observation were fewer than anticipated in the beginning of the thesis process. However, the observations made supported the choices made in designing the tool and the supporting material.

The finished tool was sent to the risk coordinators of nine sub-business units. The risk coordinators were instructed on how to use the tool in a kick-off workshop. The initial response was positive: the new tool was considered straightforward and easy to use. The formulas and functions of the tool worked as planned. The tool worked correctly. Locking the cells that were not to be edited turned out to be a good decision. One sub-business unit had attempted to fill in values that were automatically calculated and asked the writer why they cannot edit the tool. Otherwise, the risk coordinators seemed to know how to use the tool correctly.

In the business unit level workshop, risk assessment as a whole received criticism, but not the localised tool per se. The scope of different security risk domains were considered uneven and somewhat difficult to grasp. The terms ‘threat’, ‘vulnerability’, and ‘impact’ as well as the different scales were criticised for not being completely clear. However, these are established terms in the field of risk assessment. The new tool was considered a little confusing as the drop-down list had value 1 at the top and value 5 at the bottom, unlike in the value chart. This is illustrated in Figure 6. There was no other negative feedback or development suggestions that concerned specifically the new tool rather than the risk assessment in the company in general. No major shortcomings or areas to be developed were identified.



Impact
4

1
2
3
4
5

4
3
3

Impact
5 - Critical
4 - Very important
3 - Important
2 - Low importance
1 - No material impact

Figure 6: The two directions of the scales

The informal feedback from all the other security leads in the strategic business unit level risk workshop was very positive. Finland’s security lead and the writer of this thesis introduced the whole risk assessment process in Finland, including the new tool, to others. The tool was considered to be very clear and easy to use. Especially the possibility to add new identified risks was seen as an important improvement compared to the enterprise-level tool. All of the security leads wished to try out the tool, and they were asked to test it and to give more feedback and suggestions for further development and improvements. The feedback from this testing is excluded from this thesis due to time constraints.

The Security Risk Guide was seen as a useful aid because it explains threats in a concrete and simple manner and it provides supporting questions. The decision was made early on to write this guide in Finnish because the identified threats may include terminology that is not clear to everyone. Only later did the writer of this thesis realise that the sub-business unit of Estonia would have needed this guide in English. In the comments section of the risk assessment tool, the Estonian risk coordinator concluded that a description of threats would have been useful. This proved the need for the guide. In addition, the security leads requested the supporting material in English so that they could use it in their business units. Thus, the guide should be translated into English for future reference. There is a clear need for development. According to the observations made, the products appear to make the risk assessment process easier.

7 Discussion

According to the company’s security management framework, risk management is aligned with ERM, which is a holistic approach to risk management. A typical risk assessment is comprised of three stages: risk identification, risk analysis, and risk evaluation (ISO 31000:2018, 16). The local risk assessment in the case company was focused on the risk analysis phase. Risks had been identified on a higher level. However, the new tool developed during this thesis gives stakeholders an opportunity to identify new threats which are then communicated further to higher levels. If there are risks that are assessed as high or very high, a description of threats and current controls is given. This is where the local risk assessment process ends. Decisions about mitigation efforts are made on a higher level.

During the thesis process, it became apparent that the case company’s risk assessment process has some areas that might require improvement. During the literature review, it became clear that risk assessment is influenced by subjective perceptions, opinions, and judgements. Thus, assessment should always involve several stakeholders to be more objective and accurate. (Merna & Al-Thani 2010, 33.) Some sub-business unit assessments involved several stakeholders, but not all. Some assessments were completed by one stakeholder and then confirmed by another. Some assessments were based solely on one stakeholder’s view.

It seems that not everyone involved in assessing risks were sufficiently informed about all the different aspects of risk assessment. For example, the meaning of different values was not completely clear to everyone. It is worth considering whether risk workshops with security leads should be made mandatory so that an expert in assessing security risks could guide the risk coordinators throughout the process. Currently, the risk workshops offered for sub-business units are optional. Apart from the initial kick-off workshop, no sub-business unit requested risk assessment workshops. An alternative to mandatory risk assessment workshops could be a more comprehensible security risk guide which provides more information about risk assessment. The guide produced during this thesis is focused on threats. Those who assess risks should dedicate a sufficient amount of time and effort in the process. It could be considered that some of the results submitted reflected to some degree both a lack of knowledge and a lack of effort. This evaluation is based on the overly optimistic assessments and on the attitudes observed. More training could be an answer to this problem. Hopkin (2017, 316) states that one of the main reasons for training is to make sure that assessments are consistent.

Finland’s security lead has made a good effort in developing the case company’s risk assessment within his area of responsibility. The initiatives to develop a new tool to support his assessments and to organise workshops, among other things, indicate this. It is recommended that this approach could be followed in other business units. In the final workshop, where all the security leads met face-to-face, it was noted that some security leads have insufficient knowledge of the whole risk assessment process. This is partly due to lack of experience. Some final risk assessments for other business units in Northern Europe were completed just in time for the final deadline, and they were based on one person's views. More training could be considered in other business units, too.

It is recommended that the case company stresses the importance of a holistic process: starting the risk assessment from the very bottom, in the sub-business units, and making it a chain of assessments all the way to the top. There should be more cooperation horizontally between different business units. The final workshop between the security leads was beneficial, but it also proved that, first of all, cooperation needs to start earlier in the process. Some problems and solutions became apparent only shortly before the final deadline. Secondly, every risk assessment should involve at least two employees. Some risk assessments that were based on one stakeholder's view were overly optimistic. There could be two reasons for this: either those who make risk assessments are not able to make informed decisions about the threats, or the risk levels are kept low deliberately to avoid mitigation efforts. If more employees were involved in assessing risks, the results yielded would probably be more accurate.

8 Conclusions and Self-Assessment

The strategy applied was a qualitative and functional thesis. Literature review and participant observation were used to collect data, and content analysis was used to analyse the collected data. A qualitative and functional thesis was a suitable choice of strategy. The main focus of the thesis process was the concrete risk assessment tool, the Security Risk Guide, and the workshops. The approach was practical and closely tied to the business environment. The literature provided a solid background and guidance. The amount of risk management literature is so extensive that at times it was difficult to decide what should be included. Participant observation helped to transfer theory into practice and to find the right approach that would fill the case company's specific needs. Content analysis was a good way to determine how successful the products of the thesis process are.

The objective of this functional thesis was to determine how to best develop the local risk assessment methods of the case company. The purpose was that those, who represent their sub-business units, can assess security risks in an efficient and reliable manner. The intention was that with the help of these results, Finland's security lead would be able to make an accurate and realistic risk assessment of the whole business unit. The identified research question was:

> What kind of local risk assessment method would support the security lead in assessing security risks?

It can be concluded that the simplified and localised tool developed by the writer can make the risk assessment more straightforward and efficient. This is based on the feedback that the participants, especially the security leads, have given, and on the observations made. However, some of the actual results of risk assessments were considered by the security lead to be somewhat unrealistic, in other words, too optimistic. As a conclusion, the risk assessment process should still be further developed by providing training, raising awareness, and increasing cooperation, for example. The Security Risk Guide was considered useful. However, it should be translated into English for other business units. It should also be considered whether the guide should be more informative about the risk assessment in general and not be solely focused on threats. Thus, the answer to the research question is that the local risk assessment tool and the guide produced during this thesis process can support the security lead in assessing risks, but that the development of the local risk assessment process should continue after this thesis.

The strategy and the methods used in this thesis support the defined objectives well. The findings are specific to the phenomenon researched. The research question gets to the heart of the problem. The process has been described as objectively as possible. If the same research was repeated, the results should remain substantially the same. The outcomes can be considered reliable. It can be concluded that this thesis reaches sufficient levels of validity and reliability. Ojasalo et al. (2009, 48-50) state that the goals of a thesis should be morally sound, the development project is to be conducted with honesty and care, and the results must be truly applicable in practice. These rules have been followed in this thesis. The goals have been set by the case company and the writer with the best interests of the company in mind. The thesis work has been carried out as transparently and carefully as possible in the given circumstances. The result can be used to develop the case company’s risk assessment.

The objectives set by the case company have been met. The products of the thesis have been deemed beneficial and can be used as such for future risk assessments or modified for other risk assessment needs, such as other risk areas or other units. If need be, the products can be developed further to meet new requirements. The full ownership and responsibility of the products are given to the case company after the completion of this thesis. It is suggested that the whole risk assessment process should be further developed, for example, based on the recommendations given in this thesis. After this, a new research could be carried out to see how improved cooperation, more training, and compulsory workshops or perhaps a more extensive Security Risk Guide have influenced risk assessment.

Employment in the case company has been an invaluable advantage in the thesis process. Access to relevant documents specific to the company was made easy. The writer gained a good understanding of what is needed by talking and listening to stakeholders, and by just being present and observing. The scope of the security risk assessment changed in the middle of the thesis process. The products and the thesis had to be modified accordingly. The timetable seemed tight at first, but the fixed timeframe helped the writer reach their targets on time for both the risk assessment and the thesis work.

As the writer of this thesis, I am satisfied with the results. I have respected the wishes of the case company in my decisions and suggestions to improve risk assessment. I have explained the methods and the actual process as openly as possible without revealing the company's intellectual property more than is necessary. The theory of risk assessment has been sufficiently covered, bearing in mind that this project is heavily grounded in an empirical and practical approach and it focuses on the concrete products.

This thesis project has been a meaningful and interesting process. I have grown both as a security professional and as a scholar. I have learned to combine business, security, and research. My views on risk management, and on risk assessment in particular, have become more coherent and comprehensible. As the chief security officer of the case company has emphasised, security should be baked into the company strategy. It is not a separate function that can be bolted on almost as an afterthought. And risk management is part of security. A company that thrives tomorrow, will not take risks lightly today. It considers accurate risk assessment to be a factor of success.

References

Printed sources:

Burns-Howell, T., Cordier, P. & Eriksson, T. 2003. Security Risk Assessment and Control. Leicester: Perpetuity Press.

Harris, S. & Maymi, F. 2016. CISSP Exam Guide. 7th edition. McGraw-Hill Education.

Hopkin, P. 2017. Fundamentals of Risk Management. 4th edition. Kogan Page.

Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. 2013. Johda riskejä – käytännön opas yrityksen riskienhallintaan. Helsinki: Finva.

ISO 31000 Risk Management. A practical guide for SMEs. 2015. Geneva: ISO.

Jesson, J., Matheson L. & Lacey, F. 2012. Doing Your Literature Review. Traditional and Systematic Techniques. Sage.

Juvonen, M., Koskensyrjä, M., Kuhanen, L., Ojala, V., Pentti, A., Porvari, P. & Talala, T. 2014. Yrityksen riskienhallinta. Vantaa: Hansaprint.

Kananen, J. 2009. Toimintatutkimus yritysten kehittämisessä. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kananen, J. 2014a. Laadullinen tutkimus opinnäytetyönä. Miten kirjoitan kvalitatiivisen opinnäytetyön vaihe vaiheelta. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kananen, J. 2014b. Toimintatutkimus kehittämistutkimuksen muotona. Miten kirjoitan toimintatutkimuksen opinnäytetyönä? Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kuusela, H. & Ollikainen, R. Riskit ja riskienhallinta-ajattelu. Teoksessa Kuusela, H. & Ollikainen, R. (toim.) 2005. Riskit ja riskienhallinta. Tampere: Tampere University Press.

Leino, M., Steiner, M-L. & Wahlroos, J. Corporate Governance ja riskienhallinta. Teoksessa Kuusela, H. & Ollikainen, R. (toim.) 2005. Riskit ja riskienhallinta. Tampere: Tampere University Press.

Merna, T. & Al-Thani, F. 2010. Corporate Risk Management. 2nd edition. Chichester: John Wiley & Sons.

Moeller, R. 2007. COSO Enterprise Risk Management. Understanding the New Integrated ERM Framework. Hoboken: John Wiley & Sons.

Niemelä, P. Turvallisuuden käsite ja tarkastelukehikko. Teoksessa Niemelä, P. & Lahikainen A. R. (toim.) 2000. Inhimillinen turvallisuus. Tampere: Osuuskunta Vastapaino.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. Helsinki: WSOYpro.

Purpura, P. 2011. Security. An Introduction. Boca Raton: CRC Press.

Saunders, M., Lewis, P. & Thornhill, A. 2009. Research methods for business students. 5th edition. Pearson Education.

SFS-ISO 31000:2018. Risk management. Guidelines. Helsinki: Suomen Standardisoimisliitto.

SFS-OPAS 73. 2011. Riskienhallinta. Sanasto. Helsinki: Suomen Standardisoimisliitto.

Tikkanen, S., Aapio, L., Kaarnalehto, A., Kammonen, L., Laitinen, J., Mikkonen, J. & Pisto, M. H. 2009. Ammattina turvallisuus. Helsinki: WSOYpro Oy.

Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi. 2nd edition. Helsinki: Tammi.

Vilkka, H. & Airaksinen, T. 2003. Toiminnallinen opinnäytetyö. Helsinki: Tammi.

Electronic sources:

A Risk Management Standard. 2002. IRM. Accessed 26.3.2018.
https://www.theirm.org/media/886059/ARMS_2002_IRM.pdf

Brooks, D. 2009. What is security: Definition through knowledge categorization. Accessed 12.5. 2018.
https://www.researchgate.net/publication/247478178_What_is_security_Definition_through_knowledge_categorization

Enterprise Risk Management – Integrated Framework. Executive Summary. 2004. Committee of Sponsoring Organizations of the Treadway Commission. Accessed 11.4.2018.
https://www.coso.org/Documents/COSO-ERM-Executive-Summary.pdf

Havainnointi eli observointi. 2015. Koppa. Jyväskylän yliopisto. Accessed 12.5.2018.
https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineistonhankintamenetelmat/havainnointi-eli-observointi-osallistuminen-ja-kenttaetyoe

Hyvä Hallinto- ja johtamistapa (corporate governance). 2017. Riskikompassi. Uutta suuntaa riskienhallintaan. Accessed 12.5.2018.
https://riskikompassi.fi/johtaminen-riskienhallinta/hyva-hallintotapa

G20/OECD Principles of Corporate Governance. 2015. OECD. Accessed 17.4.2018.
https://www.oecd-ilibrary.org/docserver/9789264236882-en.pdf?expires=1523958632&id=id&accname=guest&checksum=B0815E7E92719C7AE01FD2EC55775421

OED. Oxford English Dictionary. 2018. Accessed 12.5.2018
http://www.oed.com.nelli.laurea.fi/view/Entry/174661?redirectedFrom=security#eid

Purdy, G. 2010. ISO 31000:2009 – setting a new standard for risk management. Accessed 12.3.2018.
http://broadleaf.com.au/resource-material/iso-31000-2009-setting-a-new-standard-for-risk-management/

Suositus listayhtiöiden hallinnointi- ja ohjausjärjestelmistä (Corporate Governance). 2003. Hex, Keskuskauppakamari & Teollisuuden ja Työnantajain Keskusliitto. Accessed 17.4.2018.
https://cgfinland.fi/wp-content/uploads/sites/39/2012/01/cg_suositus_suomi20031.pdf

Vilkka, H. 2006. Tutki ja havainnoi. E-book. Accessed 9.3.2018.
http://hanna.vilkka.fi/wp-content/uploads/2014/02/Tutki-ja-havainnoi.pdf

Unpublished sources:

Internal material about the case company. 2018. Accessed 2.3.2018.

Internal material about risk management. 2018. Accessed 7.3.2018.

Figures

Figure 1: The model for calculating risk levels (Internal material about risk management 2018) 10

Figure 2: Principles of good risk management (ISO 31000:2018, 8) 18

Figure 3: Risk management framework (ISO 31000:2018, 9) 19

Figure 4: Risk management process (ISO 31000:2018, 16) 20

Figure 5: The process flow 23

Figure 6: The two directions of the scales 30

Tables

Table 1: The five impact levels and their descriptions (Internal material about risk management 2018) 11

Table 2: Risk analysis results in the Enterprise Security Risk Assessment tool 27

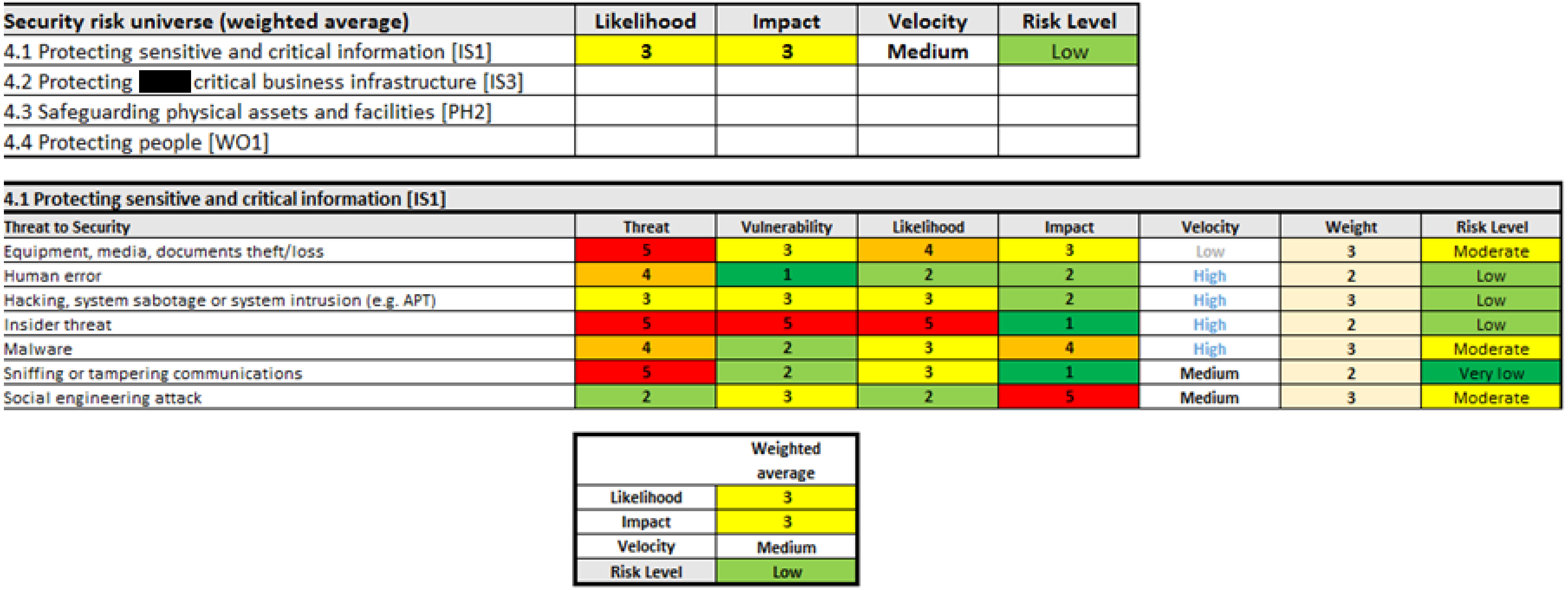
Appendices

Appendix 1: Observational checklist 40
Appendix 2: Security risk assessment tool for business units 41
Appendix 3: An excerpt of the Security Risk Guide 42

Appendix 1: Observational checklist

1. How the tool works.
2. How well the risk coordinators know how to use the new tool.
3. Possible shortcomings and areas to be developed with the tool.
4. Attitudes towards the tool.
5. The usefulness of the Security Risk Guide.
6. Possible shortcomings and areas to be developed with the Security Risk Guide.
7. How the new tool and the Security Risk Guide affect the assessment process.

Appendix 2: Security risk assessment tool for business units

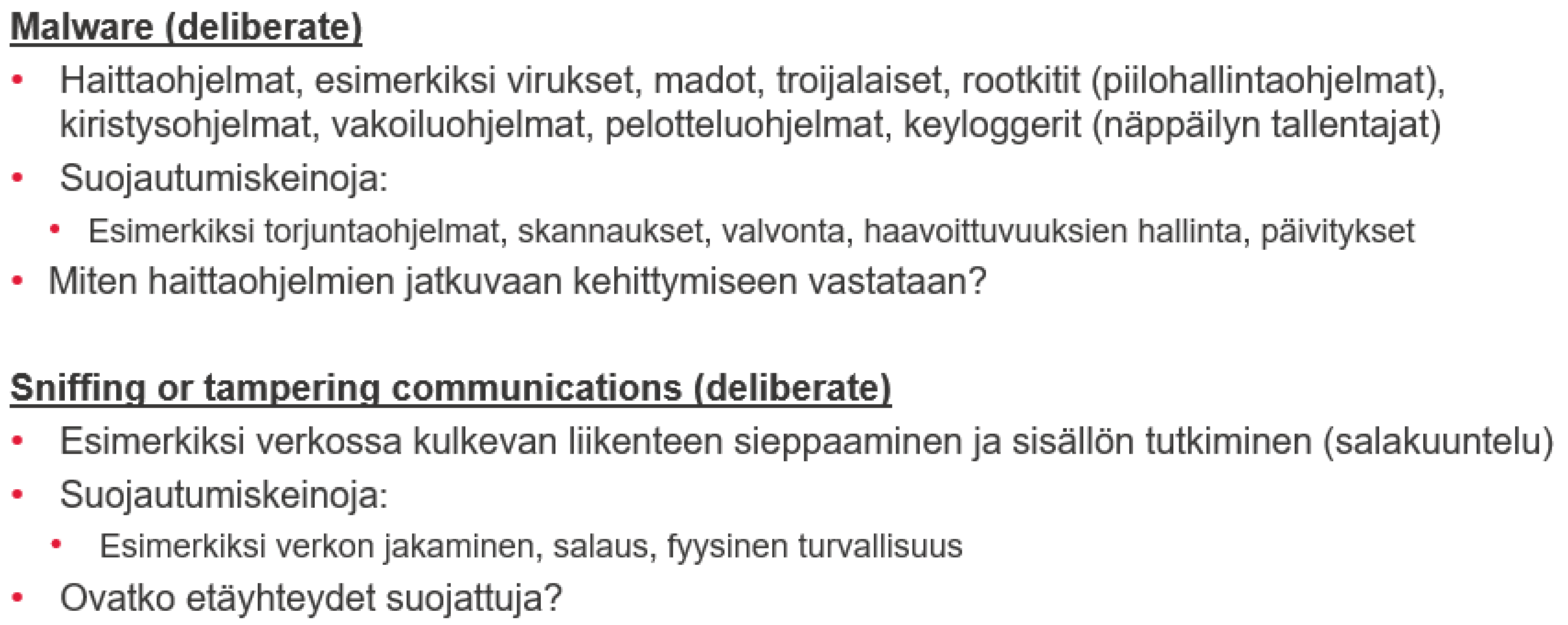


Security risk universe (weighted average)	Likelihood	Impact	Velocity	Risk Level
4.1 Protecting sensitive and critical information [IS1]	3	3	Medium	Low
4.2 Protecting [redacted] critical business infrastructure [IS3]				
4.3 Safeguarding physical assets and facilities [PH2]				
4.4 Protecting people [WO1]				

4.1 Protecting sensitive and critical information [IS1]							
Threat to Security	**Threat**	**Vulnerability**	**Likelihood**	**Impact**	**Velocity**	**Weight**	**Risk Level**
Equipment, media, documents theft/loss	5	3	4	3	Low	3	Moderate
Human error	4	1	2	2	High	2	Low
Hacking, system sabotage or system intrusion (e.g. APT)	3	3	3	2	High	3	Low
Insider threat	5	5	5	1	High	2	Low
Malware	4	2	3	4	High	3	Moderate
Sniffing or tampering communications	5	2	3	1	Medium	2	Very low
Social engineering attack	2	3	2	5	Medium	3	Moderate

	Weighted average
Likelihood	3
Impact	3
Velocity	Medium
Risk Level	Low

Appendix 3: An excerpt of the Security Risk Guide



Malware (deliberate)

- Haittaohjelmat, esimerkiksi virukset, madot, troijalaiset, rootkitit (piilohallintaohjelmat), kiristysohjelmat, vakoiluohjelmat, pelotteluohjelmat, keyloggerit (näppäilyn tallentajat)
- Suojautumiskeinoja:
  - Esimerkiksi torjuntaohjelmat, skannaukset, valvonta, haavoittuvuuksien hallinta, päivitykset
- Miten haittaohjelmien jatkuvaan kehittymiseen vastataan?

Sniffing or tampering communications (deliberate)

- Esimerkiksi verkossa kulkevan liikenteen sieppaaminen ja sisällön tutkiminen (salakuuntelu)
- Suojautumiskeinoja:
  - Esimerkiksi verkon jakaminen, salaus, fyysinen turvallisuus
- Ovatko etäyhteydet suojattuja?