Saimaa University of Applied Sciences
Faculty of Business Administration, Lappeenranta
Degree Programme in International Business

Miikka Vasenkari

Risk analysis for a medium-sized company, case Oy Saimaa Terminals Ab

Thesis 2018

Abstract

Miikka Vasenkari
Risk analysis for a medium-sized company, case Oy Saimaa Terminals Ab, 41 pages, 1 appendix
Saimaa University of Applied Sciences
Faculty of Business Administration, Lappeenranta
International Business
Thesis 2018
Instructors: Senior Lecturer Sari Jokimies, Saimaa University of Applied Sciences and Laura Hasko, Development and Quality Manager at Steveco Oy.

This thesis attempts to explore how ready-made risk registers can be adapted and utilized in a different risk environment. The thesis was commissioned by Oy Saimaa Terminals Ab and its parent company Steveco Oy. The subject of the risk analysis are three ports located in Southern Finland in Kotka (Hietanen), Hamina and Imatra.

The researcher does not have extensive background in risk management. A literary review of the subject was conducted to provide enough background to conduct the risk analysis. The core concepts of risk management are introduced along with the ISO 31000:2009 risk management standard to provide a basis for theoretical framework for risk analysis.

The results of the analysis are shown in a table with average risk magnitude comparing the results from the three ports. The results indicate that all the locations have a unique risk profile with emphasis on different risk categories. The results from the risk analysis are not generalizable across different studies and are likely to be of use only to the case company. Any major outliers in the risk categories are discussed in the results.

Risks requiring special attention for the three ports include the age of the loading equipment at Hamina, IT-security and human resources at Hietanen and machine operating safety at Imatra. Recommendations for further development of the company's risk management activities include the creation of a risk-aware culture in the organization and periodically reviewing and reassessing the risks at the ports.

Keywords: Risk management, risk analysis, risk register, ISO 31000:2009

Table of contents

1 Introduction

This chapter introduces the topic of the thesis, the case company, research objectives, a short overview of the framework used, and the structure of the thesis.

The topic of the thesis is narrowed down for the author by the company and as such there was no need to spend too much time going through other options for thesis topics. The downside of this topic is the scope of the empirical research and the challenging concepts of risk management. There will be an internal and external audit for the risk assessment later in the company and this means that the project will have real world implications beyond what is required by the university of applied sciences.

1.1 Case company Oy Saimaa Terminals Ab

The thesis is commissioned by Oy Saimaa Terminals Ab (a subdivision of Steveco Oy), a medium-sized company which operates in the shipping and logistics industry providing various services including forwarding, loading, warehousing, port and agency services in the Lake Saimaa area. The company has specialty expertise in project cargo handling.

The company operates ports in Hamina and around the lake Saimaa area in southern Finland together with the associated company Joensuun Laivaus Oy, including Lappeenranta, Imatra, Hamina and Kotka which are also the focus of the risk analysis. The field of port operation is highly competitive, and this is driving prices and profits down. There is also a high entry fee into the field as machinery and facilities are expensive and the actual operating areas (ports) are limited. The Steveco Oy group employs about 850 people with a yearly revenue of 160 million Euro.

The results from the risk assessment/risk management activities detailed in the thesis report are subject to a non-disclosure agreement as it will contain sensitive information regarding the business practices of the company.

1.2 Objectives and delimitations

The primary objective of the thesis is to create risk registers for Saimaa Terminals. The focus is on adapting existing risk registers from Steveco Oy to suit the needs of Oy Saimaa Terminals Ab. The risks covered in the registers will be limited to hazard or pure risks, risks that only have negative outcomes for the company. These risks will cover occupational, health, property, environmental risks, financial and contractual risks. The product from the thesis process will be usable risk registers for the company for internal and external auditing purposes.

The existing registers mainly omit the contractual risks category, so this should be a key focus area. Most of the control and opportunity risks will be outside the scope of the thesis as these require extensive knowledge and insight of the long-term strategies of the company, information the author will not have access to. The resulting thesis report will not be a complete guide for the company on how to organize risk management for the ports, but rather it will focus on identifying risks and giving tools for the company for evaluating them with a focus on usability and updateability.

Although risk management is an ongoing process this thesis report will resemble more of a snapshot of the state of risk in the company at the time of writing as the writer will not be involved in the project after the completion of the thesis. Recommendations will, however, be provided for updating and reviewing the risk registers in the future in the conclusions part of thesis as this is an integral part of risk management.

1.3 Research question

The main research question is “how can existing risk registers be adapted to be used in identifying risks in a different risk environment?”. To specify more clearly the intent of the research the additional research objectives are:

1. To identify the main risk categories and risks of Saimaa Terminals and to explore their potential impact on operations.
2. To expand existing contractual risks category and to identify appropriate risk responses.

1.4 Theoretical framework

Theoretical framework used in the risk analysis will be defined in the second chapter. ISO 31000:2009 risk management framework will be used as the basis, but concepts will be introduced from various authors and from other risk assessment frameworks. Theoretical framework will be constructed through literary review that will be carried out concerning some prominents authors and theories of risk management. Review of the risk management literature was necessary in order to develop the author's knowledge of the field. The theoretical framework chapter is the author's attempt at bridging the gaps between the various concepts of risk management into a condenced overview of the subject.

There are conscious omissions from the framework as the subject is too broad to be included in its entirety in the span of a bachelor's thesis. The intent is to provide a solid, if regrettably brief, background of the field to provide context where the empirical research (risk registers) is taking place in relation to the other processes of risk management.

Developing the framework quickly lead to a problem with the terminology of the field. The vocabulary of risk management can pose a challenge, as there is not one standardized set of terms used throughout the field, as the authors use risk management terms interchangeably. To assist in this, ISO Guide 73:2009 Risk management - vocabulary will be used for reference wherever terms have conflicting or unclear meanings.

1.5 Research methods

This empirical research will be a risk assessment for three ports regarding strategic, operative, financial, hazard and contractual risks. The assessment includes the creation of risk registers that will include all the previously identified risks from the risk management activities in the parent company Steveco Oy. The existing registers are modified to be more suitable for a different risk environment.

After reviewing the available research strategies, case study was selected as the most suitable. Robson (2002, 178) defines case study as *"a strategy for doing*

research which involves an investigation of a particular contemporary phenomenon within its real-life context using multiple sources of evidence". A single organization is the focus, but many subunits (different ports in this case) are used as separate units of analysis. This type of research is known as embedded case study. (Saunders et al. 2009, 147.)

Data sources for the thesis report are mainly a mix of primary and secondary data with tertiary sources providing information to locate secondary sources (books). Primary sources include the previously completed risk registers for Steveco Oy and other commentary related to their use in risk assessment as well as company reports on risk management. These are used in the empirical part of the thesis, the risk assessment. The theoretical framework is constructed with the aid of secondary data sources, mainly books and journals written by prominent authors of the field. (Saunders et al. 2009, 68-70.)

The research method adopted by the author of the thesis is mainly deductive and including elements from quantitative and qualitative methods in the data collection. The risk register includes both elements in the form of numerical data representing the risk magnitude and descriptive data of the risks obtained through interviews. The data collection must be completed in one take, and time is limited, so the structured methods of deductive research approach are important. Deductive research approach is also familiar to the author of the thesis, and with no prior experience in inductive research it could pose a risk to the completion of the thesis. The decision of the research approach affects the design choices of the author's research and may not be visible in the thesis report. (Saunders et al. 2009, 127.)

Data collection and risk identification proceeds in two steps for the risk assessment. The first step includes previously generated risk registers from Steveco Oy that will provide the main source of risk identification that will be supplemented with data collection through existing literature and during the interview process. The second step is data validation through interviews conducted in the three ports. The registers will be sent ahead of time to the relevant personnel, so they will have a chance to go through them before an informal meeting will be held to discuss the risks in detail. Employees are briefed to the subject and explained

the significance of their contribution to the project. The completed risk registers are then analyzed for the risk assessment and rating of risks.

Analysis of the risks may reveal shortcomings in the risk management practices of the company and improvements will be recommended based on the research. The resulting thesis report may form a foundation for a guide book for the company regarding risk management.

1.6 Structure of the thesis

In this chapter the basic information regarding the objectives of the research were laid out. A brief overview of the author's process of building the framework was provided. A more comprehensive framework used in the empirical research will be introduced in the second chapter and analysed part by part before continuing to the actual research in the third chapter. The third chapter will also introduce the risk register tool that will be used in the risk assessment. The risk registers used in the research are too long to be included entirely and will be added to appendices. Results chapter will summarize the findings of the research regarding the risk assessment with recommendations for future improvements.

The thesis report follows the thesis reporting guidelines established by Saimaa University of Applied Sciences (SUAS) and the Harvard system of referencing is used throughout the report.

2 Literature review and theoretical framework for risk analysis

This chapter addresses the theoretical concepts that will be applied in the risk analysis part of the thesis. The prevalent frameworks of the field will be introduced along with the key concepts of risk management that do not necessarily fit into the ISO framework but are important for the analysis. ISO 31000 risk management framework is introduced in more detail and this is also used to justify which parts are relevant for the implementation of the risk analysis and to illustrate how the risk analysis of the case company fits into the greater risk management framework. The description of the risk register used to conduct the research is introduced in chapter three after the introduction of the relevant concepts first.

There are many institutions and organizations offering risk management standards that detail the entire risk assessment process. The most well-known standards are being provided by Institute of Risk Management (IRM), Institute of Internal Auditors, Orange Book from HM Treasury (British government), ISO 31000 and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and its ERM extension framework.

The general risk management framework used in the thesis will follow the ISO 31000 guide on risk management process as this will be compliant with other ISO standards used by the company. The framework used in the thesis report is based on ISO 31000:2009 Risk management – principles and guides as this will comply with internal and external auditing in the company. The framework has been updated in 2018, but the writer does not have access to this updated material.

2.1 Understanding risk

2.1.1 Key concepts

In this subchapter are detailed important risk management concepts and terms that could not be fitted with other categories but are nevertheless helpful for defining the boundaries of the framework. Not all of these are directly relevant for the creation of risk registers but rather included in the processes of risk management and thus useful for the complete picture of the risk management process.

Risk is defined in the ISO Guide 73:2009 (p. 3) as "*The effect of uncertainty on objectives*". The effect is a deviation from the expected result and it can be either positive or negative. Institute of Internal Auditors defines risk as "*the uncertainty of an event occurring that could have an impact on the achievement of objectives. Risk is measured in terms of consequences and likelihood"* (Chartered Institute of Internal Auditors 2017).

Most risk definitions now include the fact that risk can also include a positive aspect, the upside of risk. This refers to (business) opportunities that can present themselves when engaged in activities that are deemed risky. These opportunities cannot manifest if the activity is never undertaken. This definition links risk to organizational objectives. In order to fully implement risk management processes, organizational objectives need to be clearly defined. (IRM 2010, 4.)

When considering risks, the exposure they create for the organization can be placed into two different levels. The first is the gross level of risk (also known as inherent risk), where no measures have been taken to reduce the effect or impact should the risk materialize. The second level is the net level of risk where the appropriate measures have been taken to reduce the impact of the event. This can also be called the current level of risk which might be a better term, since it implies that the risk can be treated further. Risks also have a risk target level which is defined by the board or the risk assessment team and it indicates the level of exposure that would be optimal for the organization in pursuit of its business goals. Net level of risk and target level of risk can be the same, but sometimes the target level can be significantly lower than the current net level of risk. This implies that further mitigation of the risk should be implemented for greater gains (or more effective mitigation). (Hopkin 2014, 165-166.)

According to ISO Guide 73:2009 (p. 3) **Risk management** refers to *"coordinated activities to direct and control an organisation with regard to risk"*. This definition can be expanded with the Orange Book's definition (p. 49) where all the processes in identifying, assessing and judging risks and actions taken to mitigate and anticipate them as well as monitoring and reviewing progress are included.

Defining the organizations **internal and external context** is critical for the successful implementation of risk management as risks should never be managed out of context that gave rise to them. Context is used to define the scope of the risk management program and this should be the starting point for any risk management initiative. An organizations internal context includes its internal stakeholders (management, employees), its culture, standards and capabilities as well as contractual relationships. External context includes all the local, national and international stakeholders that can affect the realization of the organizations objectives. Conducting a Political, Economic, Social, Technological, Environmental and Legal (PESTEL) analysis can reveal factors that can have an impact on an organization and its mission. (Praxiom 2018.)

In the beginning of risk management activities, it is important to define the internal and external context as well as the objectives, strategies and the scope of the risk management programme. **Risk criteria** includes defining the nature and types of events that can occur and how they can be graded, how likelihood is defined as well as the timeframe for the likelihood and consequences. (SFS-ISO 31000:2011, 39.)

Enterprise risk management (ERM) is an extension on hazard risk management programs and advocates a holistic view towards risk management that encompasses all aspects of an organization. ERM addresses value protection at all levels of an organization and is not limited to organizational core processes of traditional risk management. It could be argued that ERM is starting a trend towards a more risk-based approach to organizational management. (Hopkin 2014, 205.)

Core processes are the activities that deliver the most added value to the customer and are essential for the competitive advantage of an organization. Core processes of the organization deliver stakeholder expectations and attaching risks to these can be a starting point for a risk management initiative. (Ventureline 2018.)

According to the Institute of Risk Management, **risk appetite** can be defined as *"the amount and type of risk that an organization is willing to take in order to meet*

their strategic objectives. Organizations will have different risk appetites depending on their sector, culture and objectives. A range of appetites exist for different risks and these may change over time". (IRM 2018.)

If risk appetite is used to show the amount of risk an organization is willing to take, **risk tolerance** can show how much it can handle variation in the investment outcome. Risk tolerance can vary wildly between risks. (Investopedia 2018[a].)

Risk maturity refers to the level of integration and coordination across risk management functions. In essence this is the experience of the organization in risk management. Hopkin (2014, 116) defines these as the 4Ns of risk maturity:

> **Naïve** organization is unaware of a need for a risk management program or does not understand the value of a structured approach to risk management.
>
> **Novice** organization is aware of the benefits of risk management but has not yet implement a program effectively and is not enjoying the full benefits.
>
> **Normalized** organization has risk management as routine at all levels of the organization and the benefits are well understood if not consistently achieved.
>
> **Natural** organization has a risk-aware culture with a proactive attitude to risk management. Risk information is routinely used in decision-making and to improve processes.

Risk management is evolving rapidly and can today be considered a part of wider concept known as **governance, risk (management) and compliance** (GRC). It is a fairly new concept that covers an organization's approach to the three disciplines. GRC has been formally defined as *"the integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity"* (Mitchell 2007, 279).

GRC is a key focus area in the COSO ERM framework and although it is not covered in the ISO 31000 framework it is a central concept in the field of risk

management. *"Corporate… **governance** is the set of processes, customs, policies, laws, and institutions affecting the way an enterprise or corporation is directed, administered or controlled"* (Moeller 2011, 15).

Compliance is a key focus area also in risk management, but it can be considered also in the wider context and Moeller defines it as *"a state of being in accordance with some established guidelines, specifications, or legislation or the process of becoming so"* (Moeller 2011, p 16).

Internal control is a key focus in GRC and is defined in the COSO framework (Moeller 2011, 4) as a process designed to provide reasonable assurance regarding:

1. effectiveness and efficiency of operations
2. reliability of financial reporting
3. compliance with applicable laws and regulations

The purpose of this subchapter has been to introduce the reader to main concepts of risk management. In the following chapters the risk management processes will be introduced in closer detail.

2.1.2 Principles of risk management

There are different reasons companies are implementing risk management programs, the reasons can stem from mandatory, assurance, decision-making or effective and efficient core processes, known as the MADE2 reasons and these can affect the focus areas of the risk assessment (Hopkin 2014, 50-51).

Mandatory refers to the basic objectives of risk management that is to ensure conformity with various laws, regulations and obligations. The board and internal auditing will require **assurance** that risk management complies with the principles (PACED) detailed below. Risk management activities should also ensure that relevant information is available to assist in **decision-making** and achieve **efficient core processes** through improved implementation of strategy, tactics and operations. The underlying key principle behind risk management is that it

delivers value to the organization. According to Hopkin (2014, 50-51), the other main principles behind risk management programs are as follows:

Proportionate: Risk management activities must be proportionate to the level of risk facing the company.

Aligned: ERM activities need to be aligned with other activities and objectives in the company.

Comprehensive: Risk management activities must be comprehensive to be effective.

Embedded: Risk management activities must be embedded in the organization.

Dynamic: Activities must be dynamic to respond to changing risks.

This provides us with acronym PACED and these are also introduced in the literature of the Institute of Risk Management (IRM 2010, 6). In addition to these generic principles the ISO framework provides an expansive list of principles. According to SFS-ISO 31000:2011 (p. 40-41), an organization should at all levels comply with these principles for risk management to be effective:

a) Risk management creates and protects value.
b) Risk management is an integral part of organizational processes.
c) Risk management is part of decision making.
d) Risk management explicitly addresses uncertainty.
e) Risk management is systematic, structured and timely.
f) Risk management is based on the best available information.
g) Risk management is tailored.
h) Risk management takes human and cultural factors into account.
i) Risk management is transparent and inclusive.
j) Risk management is dynamic, iterative and responsive to change.
k) Risk management facilitates continual improvement of the organization.

As can be seen from the ISO framework, the principles of risk management are fairly universal regardless of which standard or source is used as the basis. These principles are echoed in almost all of the processes of risk management and are important to take into account when designing any risk management activity.

2.1.3 Risk assessment process

Risk identification, risk analysis and risk evaluation form the risk assessment process. During risk identification, the organization should identify all the sources of risk, their potential impact areas and consequences. The purpose is to create a comprehensive list of events (risks) that might modify the circumstances regarding the achievement of organizational objectives. During risk analysis a deeper understanding of the causes and consequences risks are developed. The probability and impact of the risks are considered and whether controls should be put in place to modify the level of the risk. Risk matrix can be a helpful tool in assisting in analysing the risks and the associated treatment methods. (SFS-ISO 31000:2011, 50-51.)

Risk evaluation should take into consideration the results of the risk analysis and the risk criteria established in the context in the treatment of risks. The most cost-effective ways to treat the inherent level of risks should be considered. Risk appetite and risk tolerance will play a part in the decision regarding the treatment of risks at this stage. It should also be noted that risk assessment is only effective if it used to inform decisions regarding business strategy. It should be a considered a starting point for risk management activities and not the complete process. (Hopkin 2014, 141.)

Risk assessment process can be considered the main topic inside the risk management framework that this thesis' research is mostly concerned with. This process will include the creation of the risk registers that will be the final output of the thesis process for the commissioning case company. On the next page is a common graph used to depict the risk management process and the supporting communication framework in an organization.

Figure 1. An alternative risk management process for ISO 31000:2009.

Figure 1 showcases an alternative visualization of the risk management process that is also known as the 8Rs (or in some cases the 7Rs) and 4Ts of risk management. This is widely introduced in the risk management literature, featured in the works of Hampton (2015, 83) and Hopkin (2014, 41).

Risk assessment process is not one-way only but in fact features information and experience feedback loop. As the company's experience grows in risk management activities, more risks can be recognized, and better treatment options can be planned.

Monitoring and reviewing risk management activities should be included in the risk management processes. Risk management activities should be regularly benchmarked against established industry best practices to improve organizational risk maturity. Reviews are normally conducted once a year but can be more frequent if necessary. The purpose of the monitoring and reviewing of the processes according to Chartered Accountants (2018) is to:

1. Ensure that controls are effective and efficient.

2. Obtain more information to improve risk assessment.

3. Identify emerging risks.

4. Detect changes in the internal and external context to determine if risk treatments should be revised.

In addition to sufficient monitoring of the risk management process, a reporting structure on risk should be established to support the continuous learning environment and to allow comparisons in the effectiveness of methods and tools employed. This also ensures that the expertise developed in the organization is not centred in a few select personnel, leaving the whole program at risk should the people change.

2.1.4 Risk identification and types of risk

Risk identification

ISO standard does not include a formal risk classification system, but classification of the risks is useful to ensure nothing will be missed in risk identification. Identifying risks can be placed into two distinct phases. Initial risk identification phase occurs when an organization that has not previously completed a structured risk identification process proceeds to examine the risks it faces. This phase can also occur for new projects undertaken by the organization. The second phase is continuous risk identification that considers changes in existing risks, whether they are still relevant and previously unknown risks that have surfaced. (HM Treasury 2004, 15.)

The simplest way to classify risks would be to group them according to their source, the component of the organization that would be affected and the eventual consequences of the risk materializing. SWOT and PESTLE analysis are an effective way to determine sources of risk within the internal and external context of an organisation. They can be completed separately but are more effective when combined. They also have the added benefit of being easily framed and understood, making risk management discussion easier between groups. (Mullerbeck 2015, 1.)

SWOT is the most common qualitative brainstorming method for risk assessment. SWOT stands for strengths, weaknesses, opportunities and threats. SWOT has the benefit that it takes into account the upside of risk, opportunities in the external environment. (Hopkin 2014, 145.)

Below is a simple SWOT matrix depicting the four categories arranged into internal and external factors as well as favorable and unfavorable factors. We can see that opportunities and threats have external origins while strengths and weaknesses are internal organizational factors. One requirement for successful completion of SWOT analysis is a clear definition of organizational objectives that are understood by all the participants. This helps place the various identified items to their respective categories. (Mullerbeck 2015, 2.)

Figure 2. SWOT matrix taken from UNICEF's guide to SWOT and PESTEL. (Mullerbeck 2015, 2.)

PESTLE (or alternatively PESTEL) stands for political, economic, social, technological, legal and ethical (environmental) and it considers risks and other issues from these categories. PESTLE can also be used as a risk classification system with a specific focus on hazard risks. (Hopkin 2014, 158-159.)

Completing a PESTLE analysis complements SWOT by identifying specific economic trends, social attitudes and technological developments and helps SWOT categorize them as either opportunities or threats. SWOT is too broad for consideration of specific trends at different societal sectors. The more complex the environment being considered, the more value completing a PESTLE analysis will provide. (Mullerbeck 2015, 3.)

Risks can arise from the strategy, tactics and operations adopted by the organization. Strategy refers to the long-term goals of the organization, tactics refer to the medium-term goals, usually projects, and operations detail the daily activities of the organization. Compliance to existing regulations and to stakeholder expectations can also be added here. Risks can belong to more than one of these categories at the same time.

Strategic risks are associated with the long-term strategy of the organization. They might arise from implementing the wrong type of business plan, poor business decisions or a failure to respond to changes in the business environment. (Businessdictionary 2018[b].)

Tactical risks refer to medium-term risks arising from implementation of projects or programmes of work designed to assist in the delivery of the business strategy of the organization. (IRM 2018, 4.)

Operational risks arise when an organization attempts to operate in a given field. These types of risks are closely related to processes, people and systems and these are the day to day activities of the organization. (Investopedia 2018[b].)

Compliance risks can be described as exposure to penalties and legal repercussions if certain laws, regulations or industry standards are not followed. This category of risks is heavily linked to the GRC and internal control concepts. (TechTarget 2014.)

Control risks are associated with the uncertainty of outcome for projects and when implementing programmes of change in the organization. The uncertainty can refer to the deviation from the expected outcome, deviation from budget or the expected benefits. A contingency fund and time extension should be included in project planning that reflects the level of uncertainty. Control risks arise because internal control systems lose effectiveness over time and fail to protect the assets they were originally assigned to. (BusinessDictionary 2018[a].)

Opportunity risks are risks that have a potential to enhance the achievement of the mission of the organization. These types of risks are usually taken in expectation of a positive return on investment. Opportunity risks usually arise from the

development of new business strategies where new opportunities in the market are spotted. Although an opportunity is spotted, seizing it might not be the correct business strategy and as such these types of risks are usually managed by the board. The risk is defined by committing resources to one opportunity while being prevented from pursuing other opportunities that might be better. (The Law Dictionary 2018.)

Risk management has its earliest roots in **hazard risk** management. These types of risks are directed towards organizational assets such as property, employees and environment. Traditionally, these types of risks were managed by purchasing insurance. Generally, organizations will have a tolerance towards hazard risks. Risk mitigation strategies including tolerate will be introduced in the next chapter. (Hopkin 2014, 37.)

It might be beneficial to separate the terms “hazard” and “risk” in this context as both can be and are used interchangeably in risk management literature. Hazard can be defined as a potential source of harm for property or people, and risk as the chance that something held valuable will be adversely affected by the hazard. (HSE 2001, 6.)

There are many ways to categorize hazard risks. They can be grouped according to the source, effect or the energy source of the hazard. Sources can also be grouped whether the risk arises from or impacts people, premises, processes or products. These are the main categories that hazard risks usually affect and can also be considered as categories of operational disruption. The categories of the operational disruption caused by the manifested risk event are not the necessarily the same where the final impact of the event is felt. The following categories can also be sources of risk and may be considered as a type of risk classification system. This classification is used as the basis for risk identification process for the risk analysis as it considers the main risk groups of the client company. (Hopkin 2014, 31-33.)

Category	Examples of disruption
People	Lack of people skills and / or resources Inappropriate behaviour by a senior manager Unexpected absence of key personnel Ill-health, accident or injury to people
Premises	Inadequate, insufficient or denial of access to premises Damage to or contamination of premises Damage to and breakdown of physical assets Theft or loss of physical assets
Processes	Failure of IT hardware or software systems Disruption by hacker or computer virus Inadequate management of information Failure of communication or transport systems
Products	Poor product or service quality Disruption caused by failure of supplier Delivery of defective goods or components Failure of outsourced services and facilities

Figure 3. Examples of disruption from 4Ps risk classification system. (Hopkin 2014, 32)

With consideration of the types of risk presented in this chapter and to bring the total amount of identified risks down and keep them relevant for the case company, the hazard risks are grouped into the following four main categories in the risk registers: Health and safety risks, environmental risks, criminal and business premises risks and contractual and compliance risks. Once the risks have been identified, it is necessary to determine the controls to put in place.

2.1.5 Risk mitigation / risk treatment

There is a conflict of terms regarding terminology when discussing hazard responses and different frameworks. ISO 31000:2009 framework uses the term risk treatment, instead of the more common risk response or mitigation (including the 4Ts) and defines treating risk *as "development and implementation of measures to modify risk"*. Under this umbrella term are listed the various options for modifying risk in the SFS-ISO 31000:2011 (p. 51) framework:

1. Avoiding the risk by deciding not to start or continue the activity.
2. Taking or increasing the risk in order to pursue an opportunity.
3. Removing the risk source.
4. Changing the likelihood or the consequences.
5. Sharing the risk with another party or parties.

6. Retaining the risk by informed decision.

These options are not mutually exclusive and one or more can be applied to any given risk.

The purpose of risk mitigation is to lessen the uncertainty associated with risk and provide a way to take advantage of opportunities that arise during these activities. There are four main responses to hazard risks in the form of tolerate, treat, transfer and terminate, commonly known as the 4Ts in risk management literature. It should be noted here that the hazard responses are usually determined for individual risks instead of a more general approach that considers groups of risk. Below is a short description of each response from the Orange Book (HM Treasury, 27-28):

Tolerate

The exposure to the risk may be tolerable without any further action. The cost of taking any action may also be prohibitively high or disproportionate to the potential benefit gained. This type of response usually corresponds to the low likelihood/low impact risks in the risk matrix.

Treat

Treating a risk is taking an action to reduce the likelihood of it materializing or reducing the impact of the risk. This is the most common response category as most risks will be treated to some level. This corresponds to high likelihood/low impact risks in the risk matrix.

Transfer

Low likelihood/high impact risks are usually transferred to a third party in the form of insurance. This type of response is suited to protecting assets and mitigating financial risks.

Terminate

Some risks cannot be treated to acceptable levels and the only action is to terminate the activity generating the risk. This is generally applicable to high likelihood/high impact risks.

Figure 4 below displays the risk mitigation strategies and acceptance levels in a matrix. Of course, in the real world there does not appear such clear boundaries between the mitigation strategies.

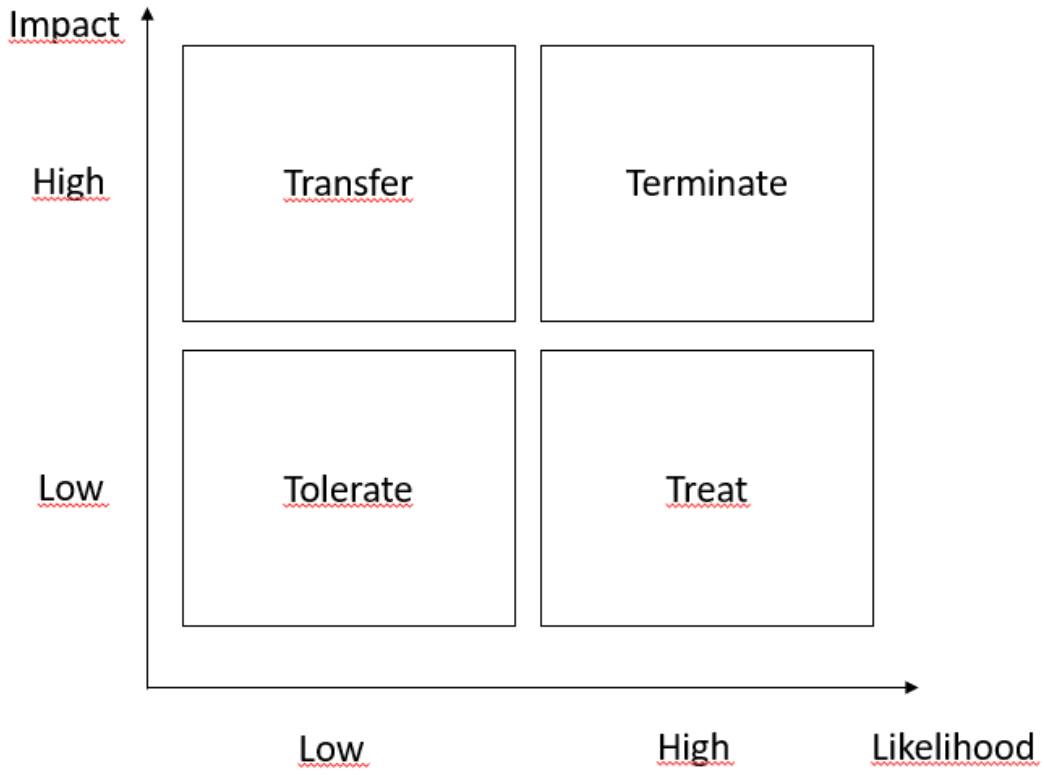

Figure 4. Risk mitigation strategies in a matrix adapted from Hopkin (2014, 234).

2.1.6 ISO 31000 framework

ISO 31000 framework provides generic guidelines on risk management that can be applied at various organizational levels from corporate to individual with a focus on ease of use. These guidelines are not tied to any specific industry and can be implemented regardless of the risk management sophistication level of the organization. The framework cannot be used for certification purposes, but it can assist in conducting internal and external auditing programmes. (www.ISO.org)

Figure 5 on the next page represents the ISO 31000:2018 version of the framework.

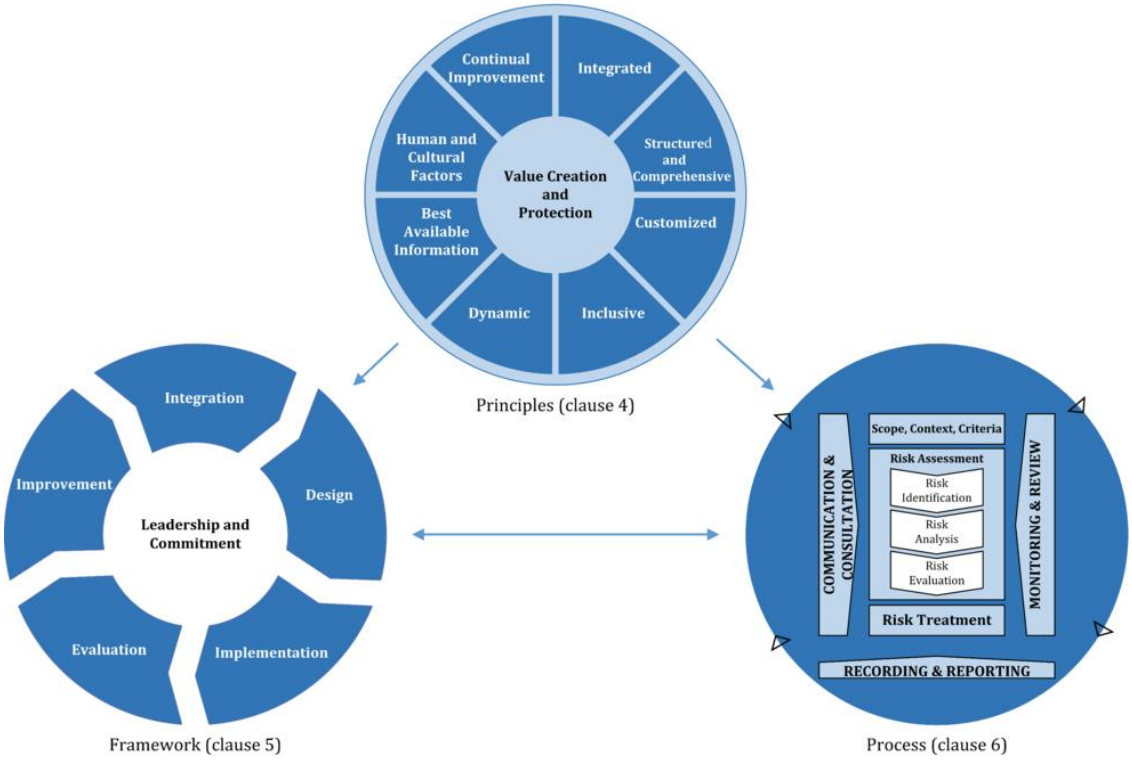

Figure 5. ISO 31000 framework (www.ISO.org)

The successful implementation of risk management will depend on the supporting framework that will assist in embedding it throughout the organization. Framework should support the risk reporting and documentation structure and ensure that the information generated through the risk management process is used in decision-making. ISO 31000:2009 framework does not provide detailed step-by-step instructions on how to achieve this but is more of a general guideline to assist management.

Risk management should be viewed as a part of the organizational processes and not a separate entity. The purpose of the framework is to support the implementation of the risk management process at all organizational levels. The starting point should be to define the internal and external context of the organization, since these can influence the design of the whole framework. The framework should include guidelines for the timeframe and strategy for implementing the framework, the training of the employees and compliance with legal and regulatory authorities. Risk management activities should be subjected to regular evaluation regarding the progress of the risk management plan and all inconsistencies should be corrected. Information from the evaluation of the risk management

framework should be used in improving the framework, processes and structure. (Hopkin 2014, 61-62.)

2.1.7 Cost of risk management

Implementing a risk management programme in an organization is never a zero-cost option. Risk management should not be considered an optional extra process from the other organizational processes. If the costs of risk management are not paid in currency they are paid in the form of unmanaged and unmitigated risk and lost opportunities. Hillson describes three levels of costs for risk management in his book *Exploiting Future Uncertainty* (2010, 41-43):

Entry costs are usually paid once by the organization when establishing a risk management capability. These include the costs incurred from training the staff and purchasing or developing the necessary techniques and tools.

Ongoing maintenance costs arise because the staff needs to be retrained in risk management to keep their knowledge up-to-date in emerging trends. New employees also need to be trained in risk management. Without constant development risk management is in danger of losing effectiveness.

Operational costs of risk management stem from assessing and addressing risk. Assessing costs arise from the implementation of the risk management programme, from time spent in risk identification workshops, in meetings or interviews and carrying out risk analyses. Addressing risk costs arise from performing risk mitigation activities to risks identified in risk analyses and generally carrying out risk response plans.

2.1.8 Benefits of risk management

Correctly implemented risk management program should provide many benefits. The most obvious benefit of risk management programs is that they will protect the assets of the organization. Being proactive (within reason) against hazard risks will be a cost-effective way of dealing with incidents. It is almost always cheaper and faster to avoid having to deal with incidents retroactively. (IRM 2010, 2.)

Also, being proactive in risk-management will increase awareness of significant risks and help discover opportunities that might otherwise be uncovered during the course of business activities when it might be too late to act on them. (Businesszeal 2018.)

Consideration of the wide range of risks an organization faces will force a long-term view regarding decision-making to management, increasing the chances that the correct business strategy will be chosen and implemented. More projects will be delivered on time, to specification and with reduced variability of results. This will improve the consistency of operations and increase brand perception. (Ten Six Consulting 2017.)

One of the greatest benefits is the accumulation of risk-management knowledge in the organization. Risk-management is rarely a one-time deal and this knowledge can be applied to other projects and business endeavours. Most of the templates and forms created for one project can be reused elsewhere with little modification. (Businesszeal 2018.)

Risk management will provide assurance to stakeholders, such as banks and insurance agencies, possibly reducing the required premiums for insurance and increasing the credit rating of the organization. It provides protection against legal action and limits liability in a lawsuit. (Chron 2018.)

Chapter two has introduced the main themes related to risk management that the author considers essential for the completion of the research. Chapter three will be concerned with the details of the execution of the empirical study as well as introducing the risk register.

3 Research methods and conducting the risk analysis

In this chapter the methods used to conduct the research and risk assessment are introduced along with justification for these choices. The main goal and the particulars of the research were given as a fairly detailed and ready-made concept to the researcher and this made the design of the risk identification and assessment much simpler. There simply was no need to spend too much time designing a valid concept for research as a part of the risk register was already completed due to prior risk management activities in the company. The second part of the chapter details the risk register used to conduct the risk identification and assessment activities.

3.1 Data gathering

From the start of the research project it was clear the research was to be carried out using deductive approach with theories based on the work of prominent authors in the field. As this researcher had little previous knowledge of the field and given the complexity of risk management it was not feasible to form theories from the findings of the risk assessment to conduct inductive research.

The focus of the risk registers was narrowed down to hazard risks as there was limited time, between 3-5 hours per port, to conduct the surveys and open interviews. This was also chosen to limit the amount of background research needed prior to these surveys as risk management is a broad subject. Taking part in these risk identification and assessment sessions were between two and four people per port. This is far from the ideal amount, but these are busy locations with busy employees, but the people who attended had extensive knowledge of their location and field of work.

This can also be considered as a form of sampling as interviewing the whole research population (all the employees at the ports) was not feasible. The results are generalized from the answers of the few participants. This shortcoming is acknowledged in the limitations of the risk assessment subchapter.

As was outlined in the first chapter, the research setting were the three ports where the risk assessment would take place. Each of the three locations had a

slightly different focus regarding the risk categories. Hietanen, the first location of the assessment, was the only port where the contractual risks were identified and assessed as the most knowledgeable person was available at this location. The contractual risks are also not bound to any specific location unlike the other categories. The other ports exclude these risks entirely as these apply to all ports equally.

The risk assessment sessions were carried out in the span of two weeks in April 2018. The actual dates were selected based on the availability of participants and it was clear this would be a problem as the locations are busy during office hours. Given the number of the participants in the sessions, it was clear this would not be a comprehensive risk assessment of the ports as more people with different specialities would be needed to achieve this. This is where the limitations of the risk categories paid off as the final categories were somewhat general risks regarding working safety in the port. Most of the risks could be analysed and assessed by all employees working in that port.

Each interview session was started with a brief introduction to the subject for the participants and their role in the risk management activities. The participants had a chance to study the risk register prior to the sessions, but there was a brief walkthrough of the main topics nevertheless to promote a discussion of the subject matter. Going through the risk register checklist was straightforward, each risk was introduced one by one and the interviewees explained if it manifested in the port or if it was irrelevant and should be removed from the risk register. The risk registers went through some modification during the sessions as some risks were better suited to other categories and some risks were found not to be relevant to any of the three ports. The researcher instructed the participants to have open dialogue regarding the risks, but in some parts guidance was needed to keep the discussion moving and relevant, and to make sure the entire risk register would be covered in the short time available at each location. All the interviews, as well as the risk registers, were conducted in Finnish as all the employees were Finnish.

Using previously generated risk registers and through the supplemental interviews, a total of 112 risks were identified across the four main categories. Some

risks were specific to a single port as not all of them carry out identical workloads. The original risk registers included many risks that were omitted as it became quickly clear during interviews that they did not apply to port operation. The original environmental risks category included a sizable amount of subcontracting and environmentally conscious leadership risks and these were beyond the scope of this research and were subsequently discarded.

In this subchapter the methods used in the research and the reasoning behind their choice were presented.

3.2 The risk register

In this subchapter the risk register concept will be introduced along with the specific risk register used in the risk assessment process for the thesis.

ISO Guide 73:2009 (p. 9) defines risk register as a *"document used for recording risk management process for identified risks".* The register should be an agreed record of the identified risks along with the controls in place and the proposed improvements. There is not a standard form for creating a risk register and they can take almost any form the users wish or require. Usually risk registers are regarded only as a part of risk management initiative in a company, but in this research, it is the main focus. On its own the risk register is just a piece of paper and not very useful. Risk register needs to be an action plan for the company regarding risk. It needs to be used to provide the intended benefits. (Hopkin 2014, 89.)

As mentioned in chapters one and three, forming the risk register did not start from scratch. The risk register used in the risk assessment has four main categories of risks namely health and safety at work, environmental risks, crime and business premises risks and contractual risks. Of these categories the environmental and contractual risks remained virtually unchanged as it became clear that the contractual risks required extensive knowledge of the shipping industry. The environmental risks ended up being more of an additional category as subcategories such as environmentally conscious leadership did not apply as the leadership is coming from higher up than the individual ports. And "green" legis-

lation also did not apply to the employees of the ports. The discussion was centred around the health and safety at work, which is understandable given that the focus of the assessment is on hazard risks and ports are hazardous work environments.

The original risk registers had more subcategories and risks (the original risk registers from Steveco Oy), but these were omitted after the identification and assessment was over as they became redundant. The final version of the risk register uses the following structure:

1. **Health and safety at work** (44 total risks identified)
    a. Occupational health
    b. Safety at work
        i. Moving in the port
        ii. Machinery and vehicles
        iii. Loading and unloading
        iv. Storage
        v. Other / Miscellaneous
2. **Environmental risks** (12 total risks identified)
    a. Chemicals and waste
    b. Emissions and malfunctions
    c. Consumption
3. **Crime and business premises risks** (33 total risks identified)
    a. IT-security risks
    b. Crime
    c. Business premises security
4. **Contract and liability risks** (23 total risks identified)
    a. Subcontracting
    b. Contracts and liability
        i. Contract terms and interpretations
        ii. Miscellaneous contracts
        iii. Contract process
    c. Liabilities
    d. Preparing for problems

More than double these risks were covered, discussed and discarded from the preliminary risk registers. Total of 112 risks were left in the risk register as relevant. This does not mean that more risks would not be identified in further risk identification sessions with additional personnel as this list is certainly not exhaustive, nor is it portrayed as such.

Risk description			Risk			Status	
No.	Subject	Event	Impact	Likelihood	Magnitude	Implemented actions	Planned actions
Health and safety at work							
1	**Occupational health**						
1.1	Sickness	Long-term absence	1	1	2	Regular health checks	
Safety at work							
2	**Moving in the port**						
2.1	Internal traffic	Driving a car	1	1	2		
Crime and business premises							
3	**Information security**						
3.1	It- systems	Suspect email	2	2	4	Staff training, precautionary actions	Updating security programs

Figure 6. Example of a risk register. The entire register used in the assessment can be found in appendix 1.

As the author is focusing mostly on hazard risks in the research, a ranking of the impact severity of risks is in order. In his book *Fundamentals of Risk Management* (2014), Hopkin defines the impact (or treated) levels of hazard risks:

Minor: A situation where a loss might hurt an operating unit but would not be visible on financial statements.
Significant: An event that can cause a reduction in current year revenues or has potential for a substantial impact on operations.
Critical: An event that prevents company's ability to conduct business.
Catastrophic loss: Destruction of majority of assets, unbearable financial loss or the immediate bankruptcy and dissolution of the enterprise.

These categories will be adapted from previously completed analyses in the organization to be used in the risk registers with risk scoring as follows:

0 No threat: Either the risk does not exist in the company or the risk does not pose a threat.
1 Minor: The event causes a passing disruption and the financial repercussions are minor. Impact can be dealt with without outside assistance.
2 Significant: The event causes greater or longer-term impact to operations or disruptions that are longer in duration, but minor in impact. The event affects external stakeholders. Subcontractors are contacted for help in containing the impact.
3 Critical: The event causes permanent or irrecoverable damage to the organization with significant financial losses. The authorities might be required to contain the impact.

The status of the risk should also be included in the form of actions in place and actions to be taken at a later date. Usually a risk register also includes a risk owner, but it was not possible to determine these in the short interview sessions. The focus was instead shifted to identifying and assessing the risks to get a baseline reading of risk status in the ports. These can be supplemented by additional risk management activities in the company later.

The register contains a description of each risk with specific risk events along with consequence and likelihood to give a magnitude to each risk. In this register the level of risk is indicated as impact + likelihood = magnitude. Risk magnitude is used in assessing whether the risk requires further action.

Risk magnitude presented as numbers:

1-2 Low: Risk can be tolerable if further reduction is too costly.

3-4 Medium: Presents a significant risk to operations and these should be mitigated to low status. Can be tolerated only if critical to operative functions and mitigation is too costly.

5-6 High: These risks have to presented to the board and action should be taken to reduce them to a lower level or eliminated entirely.

Below is a visual representation of the risk magnitude in the form of a risk matrix. These are an effective way of communicating the risk levels for different audiences as they are easy to understand regardless of the sophistication level of the audience. In this matrix green represents the score 1-2, yellow 3-4 and red the score of 5-6.

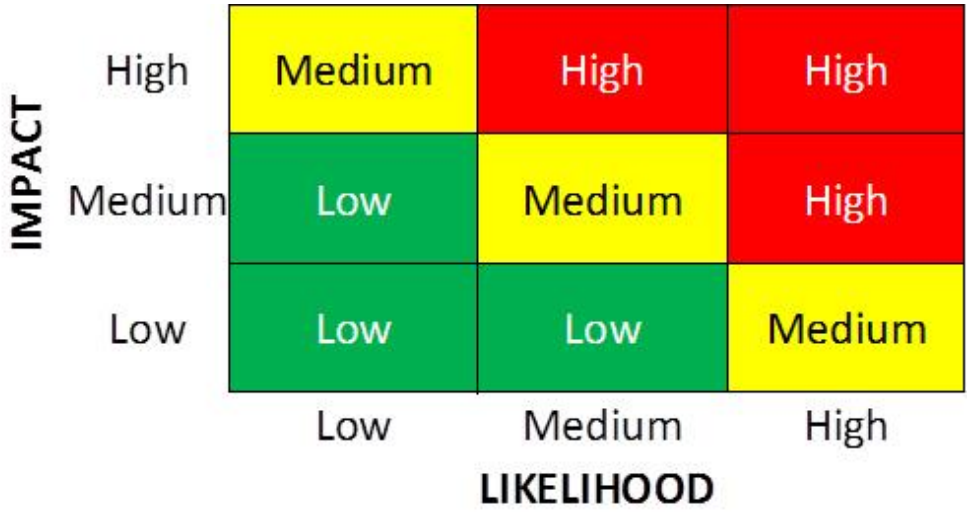

Figure 7. A simple risk matrix visualizing the overall risk level. (PivotPoint Security 2016)

There are many benefits to using a risk register in risk management. The completed register offers a clear and concise overview of the status of risk management in the organization. A well-managed risk register can be used for auditing the risk management activities of the organization as well as an aid in decision-making. Having a clear list of risks faced by the organization can also enable communication regarding risk management between the various levels of management. This can also reduce the ambiguity surrounding risk management as the abstract concepts can easily be understood when they are listed in a logical manner. One way to enable the constant updating of the register is to keep it as an open file in the intranet allowing everyone to update it regularly. (The Law Society 2017.)

While using risk registers in risk management is generally regarded as a positive activity, it is not without its flaws. Risk registers tend to portray a state of risk in the company. They might be updated once or twice in a year, but generally they are not very dynamic meaning they are only updated at mandated intervals. To drive change in the company they should be used frequently. There is also risk that managing the risk register becomes more important than managing the actual risks. Management and employees might view their part in risk management completed if they attend risk management workshops and produce the completed register, although this is certainly not true. (Hopkin 2014, 89.)

Usually a risk register does not convey the positive aspects of risk thus it can end up as a list of only negative events and might result in missed opportunities. Using risk registers can also blind the users to new threats, repeating the same risk assessment process over and over again. (Project Management Institute 2011.)

The data gathered during the risk identification and assessment will be analysed in chapter 4. This chapter has detailed the research methods used to conduct the empirical research as well as introducing the main vehicle of the research, the risk register.

4 Results of the risk analysis and further discussion

The results of the risk assessment interviews and the analysis of the risk registers will be discussed in this chapter.

As can be seen from the overview table of the risk assessment for the three ports, not all risk categories were relevant for each location. The categories and sub-categories that were not assessed are marked as “not applicable”. This marking does not mean that no risks were identified or discussed from these categories, but rather that the findings were insignificant (score 0) or that the risks were not directly relevant for that location. The risk magnitudes are represented as averages, so the results can be compared between the locations and to give the reader an idea of the overall risk levels of the categories.

HEALTH AND SAFETY AT WORK		**Hietanen**	**Hamina**	**Vuoksi**
1	**Occupational health**	2	1.8	1.67
2	**Safety at Work**			
	MOVING IN THE PORT	2	3.67	2.86
	MACHINERY AND VEHICLES	Not applicable	2.43	1
	LOADING AND UNLOADING	Not applicable	3	1.67
	STORAGE	Not applicable	3.67	2.67
	OTHER	2	3	1.34
Category average		**2**	**2.93**	**1.87**
ENVIRONMENTAL RISKS				
1	**CHEMICALS AND WASTE**	Not applicable	1.5	1.2
2	**EMISSIONS AND MALFUNCTIONS**	Not applicable	2	2.17
3	**CONSUMPTION**	Not applicable	2	2
Category average		**x**	**1.83**	**1.79**
CRIME AND BUSINESS PREMISES				
1	**IT-SECURITY RISKS**	3.78	2	2
2	**CRIME**	Not applicable	0.57	0.86
3	**BUSINESS PREMISES SECURITY**	0.34	1.34	1.67
	FIRE AND EXPLOSION HAZARD	Not applicable	2.11	2
Category average		**2.06**	**1.5**	**1.63**
CONTRACTUAL AND LIABILITY RISKS				
1	**SUBCONTRACTING**	2	Not applicable	Not applicable
2	**CONTRACT AND LIABILITIES**			
	CONTRACT TERMS AND INTERPRETATIONS	2.5	Not applicable	Not applicable
	MISCELLANEOUS CONTRACTS	2	Not applicable	Not applicable
	CONTRACT PROCESS	2	Not applicable	Not applicable
3	**LIABILITIES**	2	Not applicable	Not applicable
4	**PREPARING FOR PROBLEMS**	2.75	Not applicable	Not applicable
Category average		**2.25**	**x**	**x**

Figure 8. Overview of the risk assessment for the three ports.

4.1 Findings

Each of three locations features a different risk profile due to the different activities taking place. At Hietanen the focus of the assessment was on the contractual and liability risks and the standard port operations were left out of the assessment workshop. The other locations do not feature this contractual category. Hietanen was different also regarding the general work environment as only the office area was included in the risk assessment and not the whole port. This undoubtedly skews the scoring somewhat.

Health and safety at work

This can be considered the main category of the risk assessment both in regard to the number of risks identified and assessed and the time spent discussing the risks. Ports are dangerous working environments with large machinery and limited visibility due to containers and the risk magnitude scoring reflects this.

At Hamina the average score for all categories is much higher than the other locations so the working safety in the port should be a key focus area. Notable risks include leaking storage areas and poor lighting conditions that make working in the dark dangerous. No automated lighting is installed in the storage and the switches are in a hard-to-reach location. The age of the equipment used for loading also caused concern in the interviewees.

At Vuoksi the greatest risks were safety while operating equipment and accidents in the port area as some fatalities have occurred here in the past. The average scoring is lower than Hamina as Vuoksi port is located inside a factory area with dedicated emergency services available mitigating many categories to a lower status.

In Hietanen the lack of human resources presented the greatest risk to operations as the number of staff available is limited. The same poor visibility risks apply to Hietanen as well even if there is no loading and unloading of cargo taking place. The office is situated in the middle of the port with surrounding traffic.

Environmental risks

Environmental risks were the narrowest risk category with only 12 identified risks. Assessment was simple as no toxic chemicals are handled at any of the ports apart from fuel for the machinery. The greatest risks to environment were leaking hydraulic fluids and fuel from machinery, but a containment plan was already put in place. Birds presented a problem at Vuoksi as they can contaminate the stored goods.

Crime and business premises

All three locations are in gated and guarded port areas. The scoring reflects the mindset of the interviewees that crime is not a large risk. The gates control access to the areas around the clock. Theft is not a major concern as no currency is kept in the offices. At Hietanen the IT security risks were a larger concern than at the other two ports. More confidential files and information is kept at this location and network plays a key role for operation. The category averages do not reflect major differences with the locations (2.06, 1,5 and 1.63), but the IT-security risk subcategory for Hietanen is quite high at 3.78 and warrants special attention. At Hamina and Vuoksi the age of the buildings provided the greatest concerns as the old roofing is vulnerable to collapse.

Contractual and liability risks

Hietanen was the only location where these risks were assessed. These types of risks are complicated and require extensive knowledge of the organizational operations. The actual liability risks are overall quite low as most types of risks are insurable. The greatest risks are related to turnover as the contractual sums are large compared to the number of employees handling these. These risks include delayed payments or defaulting on payment and bankruptcy of clients. Especially bankruptcy of a key client could be devastating as the turnover is great however these risks are extremely rare as the shipping companies are usually corporations with substantial financial backing.

4.2 Limitations of the risk analysis

The results from the risk analysis should be considered in the larger context of risk management. The average risk numbers should provide a simple status check for the state of risk in the organization especially relative to one another.

There are many shortcomings and potential pitfalls in the risk analysis and assessment workshops that were conducted at the ports. First and foremost, the risk management experience of the researcher is limited and based on the overview of the prominent concepts and literary review of the subject. Also, the author is not an experienced interviewer and thus it is entirely possible that interviewees were steered too much towards similar responses especially in the later interviews by explaining too much of the risks. There is also no way to measure if the interviews were conducted in a comparable way as all three ports had a different number of participants with separate responsibility areas.

The time spent in the assessment workshops was shorter than is usually recommended the risk management literature and could potentially mean that results are somewhat rushed. The limited number of participants also means that results could be wildly different if the risk assessment was conducted a second time. This means that the generalization of the risk scores is not recommended and should be considered as preliminary.

The contractual and liability risks category was complicated, and the personal input of the researcher was limited due to the insufficient knowledge of the way contracts are handled at the organization. This relegated the role of the researcher to observer as the risk register was considered and recorded.

4.3 Recommendations

Due to the limitations of the risk assessment detailed above, it is recommended to the company that a second risk assessment be conducted to either validate or dismiss the findings reported here. This would also support the fact that risk management is a continuous process and it should not end when one risk assessment ends. These complimentary assessments can also be used to update and revise the risk register featured in this thesis report.

General recommendations and observations for Oy Saimaa Terminals Oy based on the risk assessment workshops:

Hietanen

Sufficient human resources for new and existing projects caused concern as on call duties take a toll on the employees. Compared to the other two ports the IT risks scored significantly higher at this location so more training regarding IT security is recommended to the employees. Dispersal of contractual knowledge in the company is also recommended as losing a key person would cause significant damage to the contractual process and the ability to conduct business.

Hamina

Old equipment used for loading and unloading was a significant source of risk at the port. The age of buildings also caused concern for roof collapse in case of heavy rain and for a fire hazard due to old wiring and circuitry. The lighting in the port is inadequate and access to the light switches is difficult in the dark. Motion detection sensors to activate the lights are recommended for the key areas.

Vuoksi

At Vuoksi, the majority of the discussion was related to safety around machinery and internal traffic in the port area. Limited visibility in the storage area and from the machinery itself was mentioned multiple times. Maybe the prior accidents at the port affected the assessment more than at the other locations. Recommendations to install mirrors to the blind spots in the storage to improve visibility.

At the organizational level it is recommended that the environment of a risk-aware culture is nurtured. Risk management should be integrated into the processes and objectives of the organization and clear responsibilities should be allocated. Benchmarking of the processes, accountability and rewarding should be promoted to increase operational efficiency. (IRM 2010, 6.)

4.4 Conclusions

The thesis report process began with the question “how can existing risk registers be adapted to be used in identifying risks in a different risk environment?”. The answer to this question is complicated and the writer is still not sure if this was answered definitely.

On the other hand, the additional research objectives provided a clear sense of purpose for the project and retrospectively were absolutely vital for the completion of the thesis. The existing risk registers helped in the identification of the risk categories and provided a ready-made template.

1. To identify the main risk categories and risks of Saimaa Terminals and to explore their potential impact on operations.

2. To expand existing contractual risks category and to identify appropriate risk responses.

The second objective proved more challenging than initially presumed. The contractual risks are complicated and require knowledge how contracts translate to operations and projects. In the end the category remained largely untouched from the original risk registers provided to the researcher. More research into compliance risks would have been required to provide more input into the category.

The main findings of the research include the identification of the major risks at each of the three risk analysis locations, as well as recommendations for future actions based on these findings. In the end this research is from a confined risk environment and likely only of use to the client company who commissioned the risk analysis.

The researcher had limited knowledge of the field of risk management prior to the thesis process. Conducting the literary review and constructing the theoretical framework provided a fundamental overview of the field. Leading the discussion at the risk assessment workshops was an equally excellent learning experience. A great amount of practical knowledge was acquired from conducting the risk analysis and this will be useful in projects in the working life.

I would like to thank the case company Oy Saimaa Terminals Ab and Steveco Oy for providing an excellent topic and research environment for this thesis and especially my thesis instructors Sari Jokimies and Laura Hasko for patience during the extended thesis process.

Figures

List of references

BusinessDictionary 2018[a]. Control risk. http://www.businessdictionary.com/definition/control-risk.html Accessed on 25 September 2018.

BusinessDictionary 2018[b]. Strategic risk. http://www.businessdictionary.com/definition/strategic-risk.html Accessed on 13 September 2018.

Businesszeal 2018. 4 remarkable benefits of risk management you weren't aware of. https://businesszeal.com/benefits-of-risk-management Accessed on 27 September 2018.

Chartered Accountants 2018. Monitor & review. https://survey.charteredaccountantsanz.com/risk_management/midsize-firms/monitor.aspx Accessed on 11 October 2018.

Chartered Institute of Internal Auditors 2017. Glossary. https://www.iia.org.uk/resources/ippf/international-standards/glossary/ Accessed on 27 September 2018.

Chron 2018. What benefits are gained by implementing a risk management program. https://smallbusiness.chron.com/benefits-gained-implementing-riskmanagement-program-75600.html Accessed on 27 September 2018.

COSO Enterprise Risk Management: Integrated Framework 2004. Www.coso.org. Accessed on 15 March 2018.

Hampton, J. J. 2015. Fundamentals of enterprise risk management: how top companies assess risk, manage exposure, and seize opportunity. New York: American Management Association.

Hillson, D. 2010. Exploiting future uncertainty: creating value from risk. Great Britain: Gower Publishing Limited.

HM Treasury 2004. Orange Book: Management of risk – Principles and concepts. Www.hm-treasury.gov.uk Accessed on 10 September 2018.

Hopkin, P. 2014. Fundamentals of risk management 3rd edition: Understanding, evaluating and implementing effective risk management. London: Kogan Page Limited.

HSE - Health & Safety Executive 2001. Reducing risks, protecting people: HSE's decision-making process. Great Britain: Crown.

Institute of Risk Management, A Risk Management Standard 2002 www.theirm.com Accessed on 28 September 2018.

Institute of Risk Management 2018. Risk appetite and tolerance. https://www.theirm.org/knowledge-and-resources/thought-leadership/risk-appetite-and-tolerance.aspx Accessed on 24 March 2018.

Investopedia 2018[a]. Risk tolerance. https://www.investopedia.com/terms/r/risktolerance.asp Accessed on 18 September 2018.

Investopedia 2018[b]. Tactical risk. https://www.investopedia.com/terms/o/operational_risk.asp Accessed on 22 March 2018.

IRM 2010. A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000. The Institute of Risk Management.

ISO 31000:2009 Risk Management: Principles and guidelines. Www.iso.org. Accessed on 16 September 2018.

ISO Guide 73:2009 Risk Management – Vocabulary. Www.iso.org. Accessed on 16 September 2018.

Mitchell, S. L. 2007. International Journal of Disclosure and Governance. Volume 4, Issue 4 November 2007 p. 296.

Moeller, R. R. 2011. COSO Enterprise Risk Management 2nd edition: establishing effective Governance, Risk, and Compliance processes. Hoboken: Wiley Publishing.

Mullerbeck, E. 2015. UNICEF knowledge exchange - SWOT and PESTEL. https://www.unicef.org/knowledge-exchange/files/SWOT_and_PESTEL_production.pdf Accessed on 19 September 2018.

Organisation Internationale de Normalisation (ISO). ISO/Guide 73:2009 (en) Risk Management – Vocabulary. https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en Accessed on 18 September 2018.

PivotPoint Security 2016. Why use matrix-type models for risk assessment. https://www.pivotpointsecurity.com/blog/using-matrix-models-for-risk-assessment/ Accessed on 30 September 2018.

Praxiom 2018. ISO 31000 2018 - plain English definitions http://www.praxiom.com/iso-31000-terms.htm Accessed on 21 September 2018.

Project Management Institute 2011. Top 10 mistakes made in managing project risk. https://www.pmi.org/learning/library/mistakes-made-managing-project-risks-6239 Accessed on 7 October 2018.

Robson, C. 2002. Real World Research: a resource for social scientists and practitioner-researchers. Great Britain: Blackwell Publishing.

Saunders, Lewis & Thornhill 2009. Research methods for business students fifth edition. England: Prentice Hall.

Suomen Standardisoimisliitto SFS. SFS-ISO 31000:2011. Risk management. Principles and guidelines.

TechTarget 2014. Compliance risk. https://searchcompliance.techtarget.com/definition/compliance-risk Accessed on 7 October 2018.

Ten Six Consulting 2017. 8 Benefits of risk management (beyond project control). https://tensix.com/2017/02/8-benefits-of-risk-management-beyond-project-control/ Accessed on 7 October 2018.

The Law Dictionary 2017. Opportunity risk. https://thelawdictionary.org/opportunity-risk/ Accessed on 25 September 2018.

The Law Society 2017. It's risky business without a risk register. https://www.lawsociety.org.uk/news/blog/its-risky-business-without-a-risk-register/ Accessed on 12 October 2018.

Ventureline 2018. Core process definition. https://www.ventureline.com/accounting-glossary/C/core-process-definition/ Accessed on 18 September 2018.

Appendix 1. The risk register translated to English

Risk description			Risk			Risk status	
Nro	Subject	Event	Impact	Likelihood	Magnitude	Implemented controls	Planned controls
Health- and safety at work							
1	**Occupational health**						
	Sickness						
	Physical stress						
	Workstation						
	Working posture						
	Equipment						
	Mental strain						
	Harassment at work						
	Sexual harassment						
	Written plan of action for occupational health						
	Human resources						
	Occupational health and safety						
	Substance abuse program						
	Induction and work guidance						
	Pandemic						
2	**Safety at Work**						
	MOVING IN THE PORT						
	Internal traffic						
	Visibility						
	Winter						
	Working- and safety equipment						
	Working outdoors						
	First aid						
	Safe procedures						
	MACHINERY AND VEHICLES						
	Knowledge of the equipment						
	Driver training						
	Limited visibility						
	Safe handling						
	Maintenance						
	Reporting defects						
	Accidents						
	Unauthorized use						
	LOADING AND UNLOADING						
	Load binding						
	Correct load amounts						
	Wrong lifting equipment						
	Machinery and vehicular safety						
	Place of loading, loading docks						
	Condition of the machinery						
	STORAGE						
	Safe storage, collapsing						
	Water damage						
	Fire risk						
	OTHER						
	Commuting and other business						
	Using temporary workforce						
	Traffic and transport risks						
	Indoor air / air conditioning						
	Intervening in unsafe practices and risk taking						
	Lighting						

Risk description			Risk			Risk status	
Nro	Subject	Event	Impact	Likelihood	Magnitude	Implemented controls	Planned controls
ENVIRONMENTAL RISKS							
1	**CHEMICALS AND WASTE**						
	Chemicals and chemical awareness						
	Storing and handling of chemicals						
	Fuels and petroleum products						
	Waste treatment						
	Exceptional situations						
	Birds						
2	**EMISSIONS AND MALFUNCTIONS**						
	Emissions into the air						
	Emissions into the soil and water						
	Exceptional situations						
	Noise						
3	**CONSUMPTION**						
	Energy						
	Water						

Risk description			Risk			Risk status	
Nro	Subject	Event	Impact	Likelihood	Magnitude	Implemented controls	Planned controls
CRIME AND BUSINESS PREMISES							
1	**IT-SECURITY RISKS**						
	Security of information systems, Remote work						
	Security of information systems, Monitoring of operations (disruption, disk space)						
	Security of information systems, Passwords						
	Protection of information systems Viruses, malware, spam etc.						
	Personnel activities, Training on data risk management						
	Personnel activities, Information security principles						
	Malfunction of communications and security equipment						
	Functionality of telecommunications						
	Personnel activities, unauthorized copying, disclosure of information						
	Breaching the data network						
	Data loss						
	Confidentiality of information						
2	**CRIME**						
	Risks related to property						
	Theft of equipment						
	Vandalism						
	Arson						
	Burglary at the premises						
	Personnel Security Risks						
	Misconduct and wrongdoing						
	Robbery, physical violence						
	Damage / Liability for Operations						
3	**BUSINESS PREMISES SECURITY**						
	Premises, Age of Buildings						
	Access control						
	Premises, Property history						
	Maintenance of premises						
	Damage to premises, floods and fires						
	Locking the premises						
	FIRE AND EXPLOSION HAZARD						
	Rescue plan						
	Emergency exits, instructions						
	Free movement, emergency exits						
	Fire-fighting equipment						
	Fire Safety Training						
	Electrical Equipment						
	Burning materials						
	Readiness of staff						

Risk description			Risk			Risk status	
Nro	Subject	Event	Impact	Likelihood	Magnitude	Implemented controls	Planned controls
CONTRACTUAL AND LIABILITY RISKS / SHIP CLEARANCE							
1	**SUBCONTRACTING ("The Big Picture")**						
	Subcontracting relationships						
	Contracts						
2	**CONTRACTS AND LIABILITIES**						
	CONTRACT TERMS AND INTERPRETATIONS						
	Compelling laws						
	General contract terms						
	Individual contract terms						
	Payment terms						
	MISCELLANEOUS CONTRACTS						
	Contractual coverage						
	Contractual partners						
	Long-term contracts						
	Preliminary agreements						
	Written agreements						
	Other contracts						
	CONTRACT PROCESS						
	Contractual competence of the company						
	Freedom of contract						
	Formation of contracts						
	Inspection of contracts						
	Termination of contracts						
3	**LIABILITIES**						
	Third party liability insurance						
4	**PREPARING FOR PROBLEMS**						
	Delayed payments						
	Disputes						
	Alterations						
	Selection of suppliers						
	Bankruptcy						