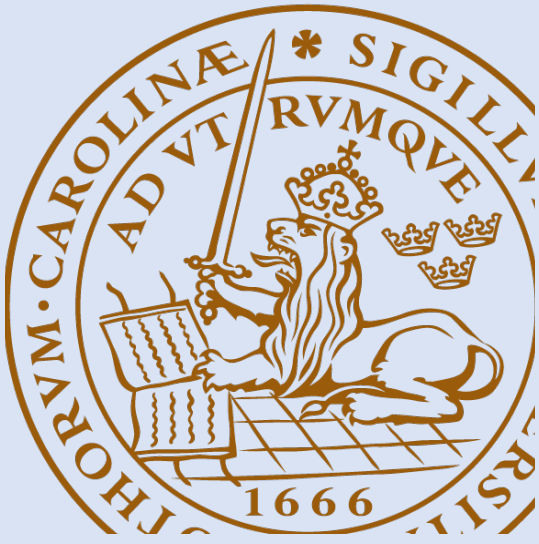
Exploring Enterprise Risk Management: A Case Study with a Global Manufacturer of High Technology Products with Operations in Sweden

Linus Hagberg | Division of Risk Management and Societal Safety | LTH | Lund University



Exploring Enterprise Risk Management: A Case Study with a Global Manufacturer of High Technology Products with Operations in Sweden

Linus Hagberg

Lund 2023

Exploring Enterprise Risk Management: A Case Study with a Global Manufacturer of High Technology Products with Operations in Sweden

Linus Hagberg

Number of pages: 64
Illustrations: 13

Keywords
Enterprise Risk Management, ERM, risk aggregation, risk consolidation.

Abstract
The purpose of this thesis is to investigate how Enterprise Risk Management (ERM), with an emphasis on risk aggregation, is conducted in practice. The thesis starts with a scoping study to review available literature on ERM. The findings from the scoping study show that literature focus on how ERM impacts certain financial variables, e.g. return on assets, return on equity, and firm value of organizations. Normative elements of ERM are also found in the literature. The findings from the scoping study further indicate a gap in the literature on risk aggregation in ERM contexts. Additional literature on risk aggregation was reviewed but in other contexts than ERM. A case study with one case company was conducted to understand how ERM is conducted in practice in a company and how ERM can be improved. The findings show that the case company has implemented ERM and have procedures in place for ERM, including procedures on aggregation of risks. Several normative elements of ERM described in literature aligns with ERM in the case company: ERM integration with strategy and objectives, organizational aspects of ERM, e.g., top management involvement, centralized ERM unit, and committees. Necessary components for successful risk aggregation found in literature (not ERM context) aligns with findings in the case company. Improvement suggestions for ERM are aimed at improving the process of selecting what risks to prioritize, increasing background knowledge in risk descriptions, and ensuring that risks have connections to events or scenarios.

Riskhantering och samhällssäkerhet
Lunds tekniska högskola
Lunds universitet
Box 118
221 00 Lund

http://www.risk.lth.se

Telefon: 046 - 222 73 60

Division of Risk Management and Societal Safety
Faculty of Engineering
Lund University
P.O. Box 118
SE-221 00 Lund
Sweden

http://www.risk.lth.se

Telephone: +46 46 222 73 60

Acknowledgements

I would like to express my gratitude to all the people who contributed to this thesis. Especially my supervisor Henrik Tehler at Lund University, and two persons from the case company.

Henrik, your guidance, advice, and ideas how to go forward during the thesis has been very appreciated.

The two persons from the case company, you know who you are. Your efforts to provide me with valuable information, inviting me to participate in meetings and making sure I received what I needed for my thesis has been very appreciated.

Thank you.

Linus Hagberg
January 2023

Summary

Enterprise Risk Management (ERM) is encompassing as the purpose of ERM, that ERM literature agrees on, is to holistically manage all risks within organizations and align risk management with corporate objectives. The purpose of this thesis is to investigate how ERM is conducted in practice and how it can be improved by conducting a case study. Three research questions were developed for the purpose of the thesis:

RQ1: What is known about ERM in the scientific literature*?*

RQ2: How is ERM conducted in practice in a company?
- With emphasis on risk aggregation

RQ3: How can ERM be improved in the case company?
- With emphasis on risk aggregation

The first research question was answered by conducting a scoping study. The online database Scopus was used to search for articles in the scoping study. The string used for Scopus searched for "ERM" or "Enterprise Risk Management" in titles, abstracts and keywords of articles only, in English, and with publication year from 2001 and onwards. The initial 6734 search hits were reduced to 70 articles by first excluding irrelevant subject areas, followed by exclusion based on titles and abstracts of the articles. The remaining 70 articles were further reduced to 40 by removing in-accessible articles and partially relevant articles. The remaining 40 articles were sorted into three groups. Articles in Group A investigated the relationship between ERM and financial indicators. However, the cause-effect relationship was not clearly established in these articles. The articles in Group B focus on normative elements of ERM, e.g. suggestions of ERM components and how ERM should be conducted. Articles in Group C had characteristics of both Group A and Group B articles. The articles in Group B and Group C provided valuable information on ERM. However, only one author (among authors from in all three groups) explicitly discussed risk aggregation in ERM. This indicates there is a gap on risk aggregation in ERM literature. Additional literature on risk aggregation, but not in ERM contexts, was reviewed and considered to be applicable in ERM contexts.

The second research question was answered by conducting a case study with one case company. The case company manufactures high technology products and thus face a variety of risks. It was decided to only include one company in the case study to enable a more thorough investigation of how ERM is conducted, compared to if multiple companies had been included. Data was collected in the case company by using documentation, interviews, direct observations, and participant observations. The findings in the case company show that processes, procedures and guidelines for ERM are in place. Numerous findings align with suggestions in literature on central aspects of ERM, e.g. top management involvement, the existence of a risk management committee, centralized ERM

team, assigned risk owners and ERM integration with strategy and objectives. Several central aspects for conducting risk aggregation in the additional literature align with findings in the case company, e.g. providing instructions, procedures, and support and the usage of common gradings.

The third research question is answered by providing improvement suggestions. This includes to investigate what impact the absence of a Chief Risk Officer (CRO) has on the company. The absence of a CRO yields longer decision paths to management compared to when there is a CRO as described in the literature. This could for example impact decision-making. The process of selecting what risks to prioritize could be improved by creating awareness of what risks that are typically over- and under managed and investigate to use additional criteria for the selection process. The background knowledge provided in risk descriptions is important to prioritize during risk reporting as it will help the ERM team to understand risks and it will also reduce uncommon categorization. Uncommon categorization makes risk aggregation more difficult. It was observed that risk descriptions varied in terms of amount and the level of details in the information provided.

It was further observed that multiple risks had weak connections to events or scenarios. Creating stronger connections to events or scenarios facilitates the understanding of risks, identification of vulnerability and risk reduction measures, impacts on other functions, and aggregation of risks. In addition to stronger connections, the events or scenarios should also be clearly defined as it leaves less room for interpretation and facilitate follow ups. If more details are provided it enables the implementation of key risk indicators as too general events or scenarios create difficulties in terms of what to measure. In risk aggregation, events or scenarios that are being aggregated should contain a certain degree of details. If not, it is difficult to trace which underlying event or scenario that realise an aggregated risk.

The findings from the case company show that risk aggregation is necessary to not overload higher management with information. It is hence of interest to conduct further research on risk aggregation in ERM.

Sammanfattning

Enterprise Risk Management (ERM) är ett omfattande begrepp eftersom det syftar till, vilket det mesta av litteraturen är enig om, att på ett holistiskt vis hantera alla risker inom en organisation och se till att riskhanteringen överensstämmer med organisationens mål. Syftet med denna uppsats är att med en fallstudie undersöka hur ERM bedrivs i praktiken och hur det kan förbättras. Tre forskningsfrågor togs fram med hänsyn till uppsatsens syfte:

RQ1: Vad är känt om ERM i den vetenskapliga litteraturen?

RQ2: Hur bedrivs ERM i praktiken på ett företag?
- Med tyngdpunkt på aggregering av risk

RQ3: Hur kan ERM förbättras på företaget i fallstudien?
- Med tyngdpunkt på aggregering av risk

För att besvara den första forskningsfrågan genomfördes en scopingstudie med hjälp av databasen Scopus. Strängen som användes på Scopus sökte efter ”ERM” och ”Enterprise Risk Management” bland titlar, sammanfattningar och nyckelord. Endast litteratur av typen artiklar, på engelska, och med publiceringsår från 2001 och framåt inkluderades. Sökningen resulterade i 6734 artiklar som reducerades till 70 artiklar genom att först exkludera irrelevanta artiklar baserat på ämnesområde, följt av exkludering baserat på irrelevanta titlar och sammanfattningar. De resterande artiklarna reducerades från 70 till 40 artiklar genom att exkludera oåtkomliga artiklar samt endast delvis relevanta artiklar. Dessa 40 artiklar delades in i tre grupper baserat på deras innehåll. Artiklar i Grupp A undersöker förhållandet mellan ERM och finansiella indikatorer. Dock är inte orsak-verkan sambandet fastställt i dessa artiklar. Artiklarna i Grupp B innehåller normativa element kring ERM och föreslår vilka aspekter som är centrala inom ERM. Artiklarna i Grupp C passar in i både Grupp A och Grupp B och blev därför tilldelade en egen grupp. Uppdelning i grupper gjordes för att underlätta sökandet efter normativa element inom ERM, d.v.s. bland artiklar i Grupp B och C. Av författarna bakom alla artiklarna i dessa tre grupper är det endast en författare som explicit diskuterar riskaggregering inom ERM. Detta indikerar att det saknas forskning om riskaggregering inom ERM. Ytterligare litteratur inom riskaggregering, fast inom andra områden än ERM, granskades och ansågs vara applicerbart även inom ERM.

Den andra forskningsfrågan besvarades genom en fallstudie bestående av ett företag. Företaget tillverkar högteknologiska produkter och står därför inför en mängd olika risker. Endast ett företag inkluderades i fallstudien för att ha möjlighet att genomföra en mer djupgående undersökning om hur ERM bedrivs i praktiken, jämfört med om flera företag hade inkluderats. Data insamlades genom dokumentation, intervjuer, direkta observationer samt observationer från deltagande. Insamlade data från fallstudien visar att processer, procedurer och riktlinjer för ERM är implementerade. Vidare är insamlade data i linje med de rekommendationer som hittats i scopingstudien, exempelvis att det finns en riskhanteringskommitté, en centraliserad ERM enhet, riskägare, och integrering av ERM med företagets strategier och mål. Även riskaggregering i företaget är i linje med rekommendationer i scopingstudien, till exempel att

förmedla instruktioner och procedurer, stöttning, tillhandahålla information, och att använda en enhetlig gradering av risker.

Som ett resultat av forskningsfråga tre ges ett antal förbättringsförslag. Ett av förbättringsförslagen är att företaget undersöker hur det påverkas av att inte ha en Chief Risk Officer (CRO). Avsaknaden av en CRO innebär längre beslutsvägar till ledningsgruppen jämfört med vad som beskrivs i litteraturen när det finns en CRO. Detta kan till exempel påverka beslutsfattande. Processen kring urvalet av vilka risker som skall prioriteras och således vidarebefordras inom företaget kan förbättras genom att skapa medvetenhet om vilka risker som tenderar att få för stort fokus inom riskhanteringen och vilka som tenderar att få för lite fokus. Bakgrundsinformationen om risker som inkluderas i riskinformationen är viktigt att prioritera under riskrapporteringen eftersom den hjälper ERM enheten (och även andra) att förstå risker och kan även bidra till att minska olikheterna i riskbeskrivningarna. Olikheter i riskbeskrivningar medför att riskaggregering blir svårare. Det observerades att riskbeskrivningarna varierade mycket med avseende på innehåll och detaljrikedom.

Det observerades även att flertalet risker hade svaga kopplingar till händelser eller scenarier. Att skapa starkare kopplingar till händelser och scenarier hjälper till att bättre förstå risker, att identifiera riskreducerande åtgärder, påverkan på andra funktioner, och att aggregera risker. Förutom att skapa starkare kopplingar, bör händelser och scenarier även vara tydligt definierade eftersom det begränsar utrymmet för tolkningar och underlättar uppföljningar. Fler detaljer underlättar implementering av riskindikatorer eftersom alltför generella händelser och scenarier är svåra att mäta. Inom riskaggregering bör händelser och scenarier som aggregeras innehålla en viss nivå av detaljer eftersom det annars är svårt att följa vilken underliggande händelse eller scenario som utlöser en aggregerad risk.

Insamlade data från företaget i fallstudien visar att riskaggregering är nödvändigt för att högre ledningen inte ska bli överväldigade med information. Det är därför av intresse med vidare forskning om riskaggregering inom ERM.

Table of contents

List of Figures

List of Tables

List of Acronyms

CEO	Chief Executive Officer
CFO	Chief Financial Officer
CRO	Chief Risk Officer
EBIT	Earnings Before Interest and Taxes
EM	Executive Management
ERM	Enterprise Risk Management
HR	Human Resources
KPI	Key Performance Indicator
KRI	Key Risk Indicator
PRM	Personal Risk Management
R&D	Research and Development
RC	Risk Committee in the case company
ROA	Return on Assets
ROE	Return on Equity
RQ	Research Question
RVA	Risk and Vulnerability Assessment
SEK	Swedish Krona
TRM	Task Risk Management

1 Introduction

This chapter starts with an introduction to the concept of Enterprise Risk Management (ERM), followed by the purpose and research questions of the thesis. Lastly, delimitations of the thesis are presented.

1.1 Background

Organizations are facing numerous types of risks on a daily basis. Events internally in organizations or externally in the environment can lead to risks. The financial crisis in 2007-2009 showed that no industry is immune to insufficient or unsuitable risk management (Brown et al. 2009). ERM is utilized by companies as protection against all the risks that occurs from running an organization (Burnaby & Hass, 2009).

Enterprise risk can be seen as a measure of how much the outcome deviates from the objectives of organizations (Dickinson, 2001). Risk management as a part of decision-making processes in companies is traceable back to the late 1940s and early 1950s, but ERM as a concept emerged in the mid-1990s (Dickinson, 2001). The popularity of ERM is a response to the increasing pressure on organizations to manage risks holistically (Lundqvist, 2014).

ERM is not unanimously defined in the literature. The purpose of ERM according to Dickinson (2001) is to manage all risks that a company faces in a systematic and integrated approach. The aim of ERM is to adopt a holistic view of risks instead of looking at risk management from a silo-based perspective (Mensah & Gottwald, 2016). The portfolio view of risks is central in ERM (Kallenberg, 2009; Jankensgård, 2019; Lundqvist, 2014; Fraser & Simkins, 2016).

Many companies struggle with ERM implementation and there are many misconceptions about ERM (Fraser & Simkins, 2016). Multiple frameworks for ERM implementation have led to uncertainties regarding what the essential components of ERM are (Lundqvist, 2014). One component of ERM is risk aggregation which refers to mechanisms that are utilized to ensure that information of high quality about risk is aggregated in a comprehensible and suitable format at the right time (Jankensgård, 2019).

This thesis explores how ERM is conducted in practice, with focus on risk aggregation, and how it can be improved by utilizing the scientific literature on ERM.

1.2 Purpose and Research Questions

The purpose of this thesis is to investigate how ERM is conducted in practice, with an emphasis on risk aggregation, and how ERM and risk aggregation can be improved. Three research questions are developed for the thesis:

RQ1: What is known about ERM in the scientific literature?

It is essential to understand what is known about ERM in the literature. The focus is to search for normative elements of ERM, e.g. how it should be conducted.

RQ2: How is ERM conducted in practice in a company?

- With emphasis on risk aggregation

Since ERM appears to be complex yet important to conduct, it is interesting to see how ERM is conducted in practice. It is presumed that companies identify numerous risks, and it seems implausible to manage all identified risks without aggregation. It is hence interesting to investigate how risk aggregation is conducted in practice.

RQ3: How can ERM be improved in the case company?

-With emphasis on risk aggregation.

It is interesting to see how the literature on ERM can be utilized to improve ERM in the case company.

1.3 Delimitations

The literature in the scoping study is collected only from the database Scopus. Furthermore, limitation is made to one single case company to answer RQ2 and RQ3. Including several companies would yield more representative findings for companies in general compared to only investigating ERM in one company. However, it is considered as implausible to investigate ERM thoroughly in multiple companies simultaneously given the resources and time available for the thesis. The decision is hence made to only include one case company. Yet, the selected case company is one of the larger manufacturing companies of high technology products in Sweden and with sales worldwide, hence making the findings interesting from an ERM perspective.

2 Methodology

This chapter is divided into two main parts: one part for the scoping study and one part for the case study. RQ1 was answered by conducting a scoping study. RQ2 was answered by conducting a case study, and RQ3 was answered by combining the answers from RQ1 and RQ2.

2.1 Scoping Study

The review of available literature is conducted by using the methodology of a scoping study. According to Arksey and O'Malley (2005), a scoping study is one of many methods that can be used for literature reviews. The authors provide four common reasons when a scoping study may be conducted in the field of interest; (1) to map available research, (2) to understand if a systematic review has the potential to yield valuable results, (3) to summarize the available research more in detail, and (4) to identify in what areas research is missing.

Arksey and O'Malley (2005) further present a methodological framework for conducting scoping studies. The framework consists of five stages:

1. Identifying the research question
2. Identifying relevant studies
3. Study selection
4. Charting the data
5. Collating, summarizing, and reporting the results.

The methodology of the scoping study in this thesis is based on the first four steps.

2.1.1 Identifying the Research Question

There are aspects that should be considered when the research question is formulated. If definitions of the included parameters in the research question are wide, many references will be generated and on the contrary, if definitions are narrow, relevant articles could be left out (Arksey & O'Malley, 2005). The recommendation from the authors is to start with wide definitions and overview the yielded references and subsequently adjust parameters. Following their recommendation, the starting point in the scoping study was to formulate a wide research question:

RQ1: *What is known about ERM in the scientific literature?*

Furthermore, limiting the search to specific areas within ERM yielded few search hits in Scopus, thus making it difficult to find literature on specific areas in ERM (described under "Search query identification"). From that point of view, it was beneficial to start wide by searching for "Enterprise Risk management" and "ERM". The following sections further describe how the scoping study was conducted.

2.1.2 Identifying Relevant Studies

Beerens and Tehler (2016) conduct a scoping study and suggest how to identify relevant articles. This step is conducted based on their suggestions where distinction is made between database selection and search query identification.

Database Selection

The database selected for this scoping study is Scopus, owned by Elsevier. Scopus indexes an extensive number of articles in several subject areas, including the relevant ones for ERM.

Search Query Identification

Scopus enables the possibility to use search strings. In line with Beerens and Tehler (2016), a search string based on Boolean algebra was developed, displayed in Figure 2.1. Since ERM and Enterprise Risk Management is used interchangeably in the literature, the string was designed to search for "ERM" or "Enterprise Risk Management". If the two were combined with an additional keyword, the number of search results became limited, e.g., if combined with "risk aggregation", the search string yielded ten search hits. The search string was designed with inclusion and exclusion criteria:

Inclusion Criteria

- Publication type is articles only
- Full text and in English only
- Published after year 2000

Articles were selected as they are peer-reviewed according to Scopus policy. The search string yielded 6734 articles with the inclusion criteria.

Exclusion Criteria

- Subject areas considered irrelevant to ERM (in Appendix A)

The subject areas that were considered irrelevant to ERM are displayed in Appendix A. The exclusion of subject areas reduced the search results from 6734 to 1177 number of articles.

2.1.3 Study Selection

The next step to further limit the search results was by reading the titles and abstracts to exclude irrelevant articles. Inclusion and exclusion criteria were utilized for the title and abstract analysis:

Inclusion Criteria

- General context, applicable on several sectors, organizations, and countries
- Specific contexts must be similar to the case company

The contexts must be similar to the case company to utilize conclusions and/or recommendations on how ERM should be conducted.

Exclusion Criteria

- General context but not applicable on the case company, e.g. large amount of organizations in numerous sectors in Malaysia
- Too specific context and hence difficult to apply elsewhere
- Irrelevant for the purpose of the thesis

The inclusion and exclusion criteria were the same for the title analysis and the abstract analysis. The reason is that numerous articles appeared relevant when the title was read, but reading the abstract showed that the article was irrelevant by applying the same criteria. For example, titles could indicate that articles were relevant, but the abstract stated that only organizations in Ghana or only small firms in the insurance sector were considered. In some articles, this was evident by reading the title and in some articles the abstract had to be read to conclude that the article was not applicable on the case company. Examples of excluded articles that were considered as difficult to apply on the case company is an article investigating the relationship between ERM and IT security, focusing on financial institutions licensed by the Central Bank of Ghana. Another excluded article proposed an ERM model specifically for the banking sector.

Articles considered irrelevant were in the wrong subject area and were included in the search results for unknown reasons. Applying the inclusion and exclusion criteria on the title analysis yielded 344 articles. The abstract analysis reduced the number of articles from 344 to 70.

Among the remaining 70 articles, seven articles were not accessible for reading and thus removed. The remaining 63 articles were read in their entirety to determine their relevance. Ten of the remaining 63 articles were excluded as they were irrelevant and should have been removed during the exclusion on abstracts but were saved for unknown reasons. Of the remaining 53 articles, 16 articles were considered as only partially relevant and had to be excluded due to time constraints.

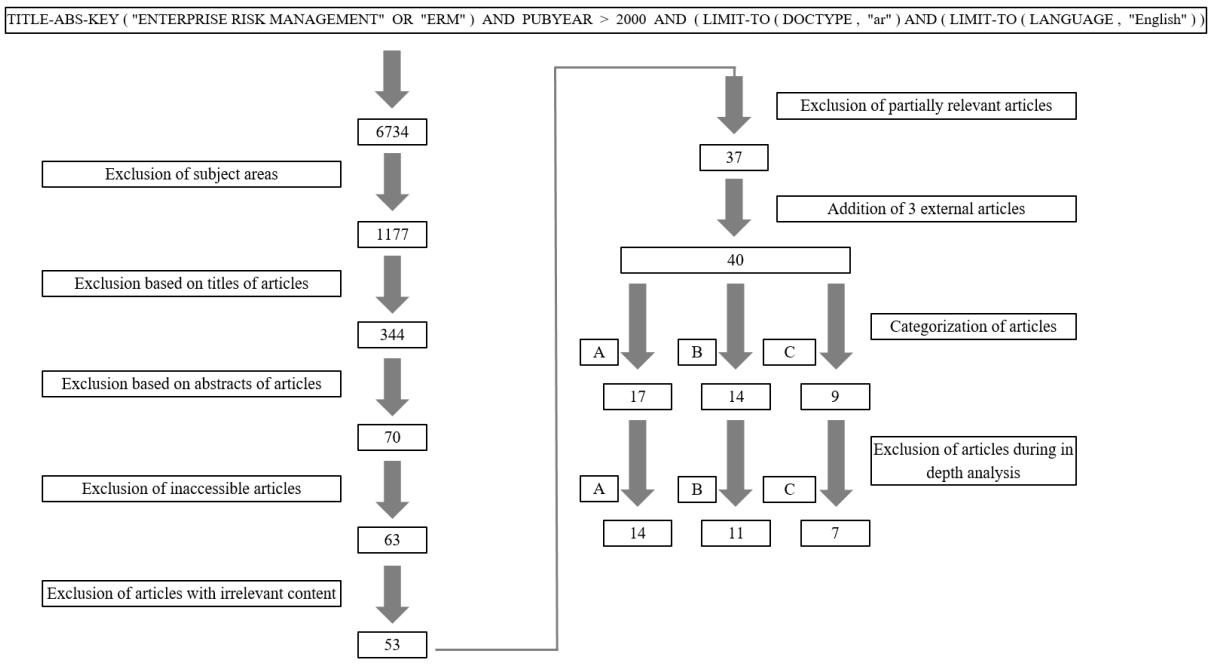


Figure 2.1. The study selection process in the scoping study.

Three external articles that were not found in the scoping study were added as their content was valuable. One of the articles was indexed as a book chapter (for unknown reasons) and thus not found since the search string was restricted to articles. However, this article had the second most citations which indicates its relevance to ERM. The second article was not found by the search string as "ERM" or "Enterprise Risk Management" were not in the title nor in the abstract. The third article added was COSO (2004) and was not indexed by Scopus.

2.1.4 Charting the Data

The process of charting the data is based on Beerens and Tehler (2016) where an overall analysis was conducted, followed by an in-depth analysis.

Overall Analysis

The remaining 40 articles were categorized into Group A, B, or C depending on their content. The articles in Group A investigate impact of ERM, or certain aspects of ERM, on specific parameters in a population of organizations. The articles in Group B suggest how ERM should be conducted by providing models and/or advice. Some of the articles covered the characteristics of both Group A and Group B and were categorized into a third group, Group C. The purpose of the categorizations was to facilitate the search for suggestions on how ERM should be conducted, i.e., articles in Group B and Group C.

In-Depth Analysis

In the final step of the study selection, three articles in Group A, three articles in Group B and two articles in Group C were excluded. What these articles had in common was that they were not as relevant as the remaining articles. It must be emphasized that they were not considered irrelevant, just not as relevant as the others. This exclusion was conducted to ensure there was enough time to thoroughly analyse the remaining articles.

2.2 Additional Literature

A decision was made to review more literature as information on risk aggregation was limited in the scoping study. Backward snowballing was used to find additional literature on risk aggregation. Backward snowballing is a technique to find additional literature by using reference lists in literature (Jalali & Wohlin, 2012).

2.3 Case Study

A case study was conducted to answer RQ2. The case company selected for the case study is interesting from an ERM perspective as the company manufactures high technology products and hence face a variety of enterprise risks. The company is described in section 5.1.

2.3.1 Data Collection

According to Yin (2003), there are six sources of evidence that are commonly used in case studies: documentation, archival records, interviews, direct observations, participant observations and physical artifacts. As the sources are complementary, combining the sources and using as many as possible is recommended (Yin, 2003). The sources of evidence used in this thesis are documentation, interviews, direct observations, and participant observations.

Meetings and workshops were used for direct observations and participant observations:

- Three RC meetings (see section 5.3 for explanation)
- Two ERM core team meetings (see section 5.3 for explanation)
- Full day consolidation workshop
- Review sessions with the ERM team

Different documentations were used for data collection:

- Organizational charts
- Written guidelines and procedures
- PowerPoint presentations
- Excel lists

One semi-structured interview was conducted with a risk manager in one of the functions to get the function perspective of their internal risk reporting process.

3 Scoping Study

The scoping study is conducted to answer RQ1. In section 3.1, results are presented from the overall analysis of the literature in the scoping study. The remaining sections, apart from the last section 3.11, constitute the in-depth analysis of the literature.

3.1 Overall Analysis

The majority of the articles with the most citations are Group A articles as illustrated in Figure 3.1. This can be interpreted that the interest is higher for articles that investigate whether ERM has proven effects compared to how ERM should be conducted. Alternatively, the interest could be to understand what ERM has effect on.

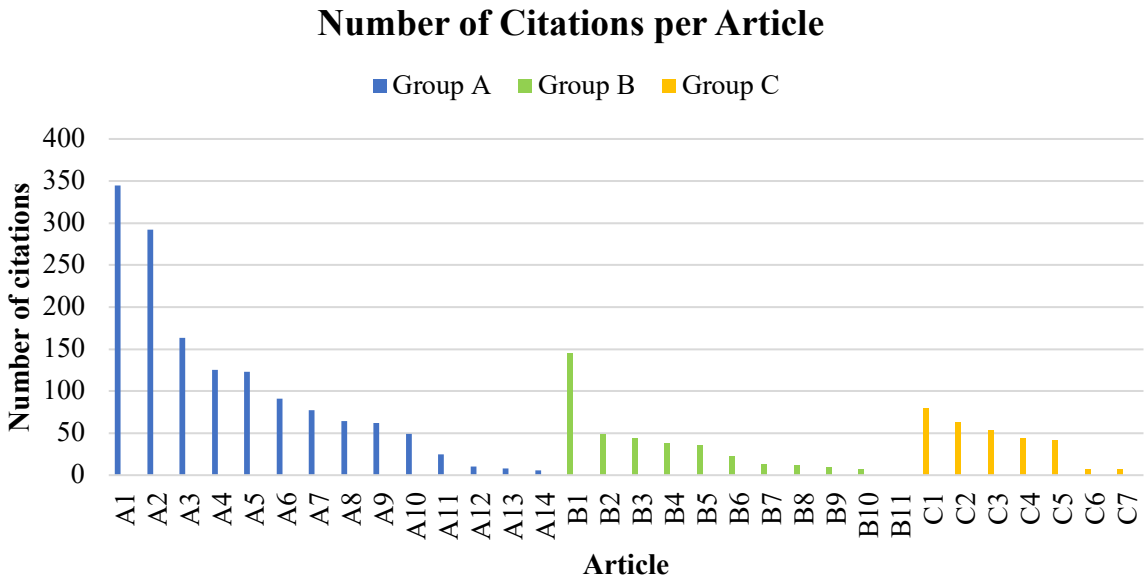


Figure 3.1. Number of citations per article.

The publication years of the articles is presented in Figure 3.2. The search string included articles published after year 2000.

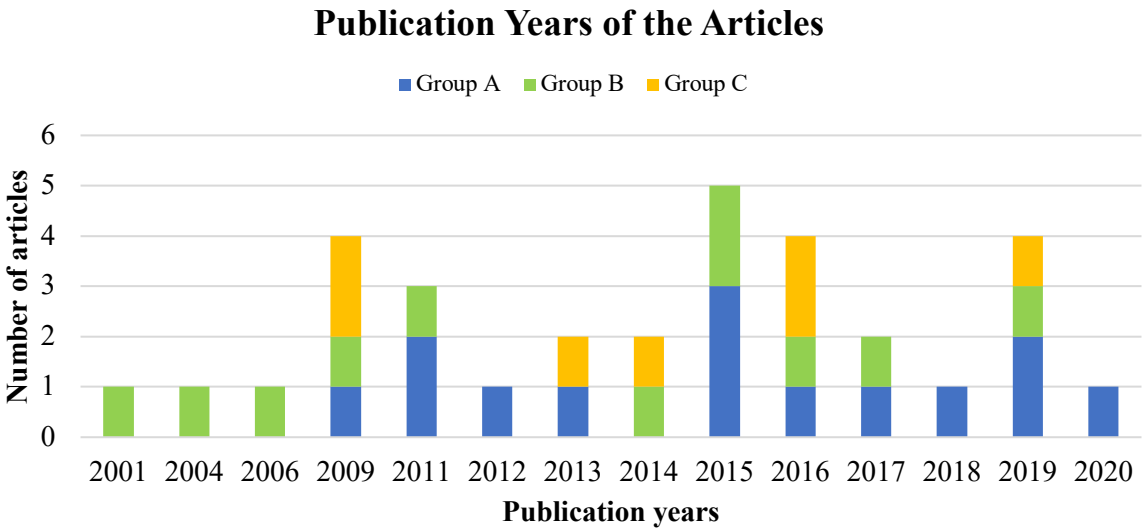


Figure 3.2. Publication years of the articles.

Only three articles were published before year 2009 compared to 29 articles published in 2009 or later. The explanation to this could be that the interest for ERM increased after the financial crisis in 2007-2009. Perhaps the most interesting question after the financial crisis was how ERM benefits companies, hence an increasing interest for the types of articles as in Group A.

3.2 Structure of the In-Depth Analysis

The in-depth analysis starts with section 3.3 presenting the definitions of ERM in the articles in the scoping study. Section 3.4 summarizes the articles in Group A. The remaining sections of chapter three present the findings from articles in Group B and Group C. The articles from Group B and Group C are presented more in detail, compared to the articles in Group A, as articles in these groups contain normative elements of ERM.

3.3 Defining Enterprise Risk Management

There is no single definition of ERM in the articles. Different definitions and descriptions of ERM is presented in this section. Dickinson (2001, p. 360) states that ERM as a concept emerged in the mid-1990s and define ERM as:

"*… a systematic and integrated approach to the management of the total risks that a company faces*".

Dickinson (2001) further elaborate on ERM and explains that enterprise risk is a measure of how much the outcome from the strategy differs from the corporate objectives.

The Committee of Sponsoring Organizations (COSO) is a recognized organization regarding ERM. COSO (2004, p. 2) defines ERM as:

"*[…] a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."*

Aven and Aven (2015, p. 1708) claim that:

"*ERM is about managing all of the organization's risk related to its activities in the value chain*".

Malik et al. (2020, p. 3) states that:

"*ERM consists of methods and processes through which organisations manage risks and capture opportunities consistent with their strategic objectives*".

Drew et al. (2006, p. 128) argue that:

"*Enterprise Risk Management (ERM) refers to a broad approach to risk management that includes strategic risk management*".

The primary purpose of ERM appears to be, by combining the different definitions, to enable organizations to achieve their objectives by managing all risks and opportunities they are facing.

3.4 Effects of ERM

The detailed analysis of articles in Group A is presented in this section. The articles in Group A mainly focus on investigation of the effects of ERM.

3.4.1 Firm Value

Hoyt and Liebenberg (2011) conclude that there is a positive relationship between firm value and the use of ERM. The results from McShane et al. (2011) show a positive relationship between increasing levels of traditional risk management capability and firm value, but no further increase in value for firms with higher ERM rating. The authors suggest that implementation of more sophisticated traditional risk management increases firm value, while achieving ERM do not. Gatzert and Martin (2015) utilize existing quantitative literature and concludes that the reviewed studies, to some extent, show a positive relation between ERM shareholder value or performance. Farrell and Gallagher (2015) conclude that there is a relationship between ERM maturity level and firm value where firms with mature levels of ERM display higher firm value of around 25 percent. ERM maturity is divided into seven themes and valuation effects due to individual attributes are seen in five of these themes whereas two themes show no relation (Farrell and Gallagher, 2015).

3.4.2 Firm Performance

Gordon et al. (2009) investigate 112 firms and conclude that the relationship between ERM and firm performance (one-year excess stock market return to shareholders) depends on how well contextual variables for the firm is matched with ERM. The investigated variables are environmental uncertainty, industry competition, firm size, complexity, and monitoring the board of directors.

Baxter et al. (2013) find a relationship between higher performance (accounting returns and Tobin's Q) for firms that invest in higher quality ERM. The authors believe this is because mitigating losses and exploiting opportunities is facilitated by higher quality ERM. Firms with higher ERM quality are anticipated by market to have better future performance. Callahan and Soileau (2017) find a positive association between ERM process maturity and operating performance measured by Return on Assets (ROA) and Return on Equity (ROE). Farrell and Gallagher (2019, p. 625) claim that their empirical evidence "demonstrates a clear link between ERM maturity and improved performance outcomes, be those outcomes measured by accounting-based parameters (ROA) or forward-looking market based measures (Tobin's Q)".

Grace et al. (2015) investigates what aspects of ERM that adds value by linking a survey of ERM practices conducted by the firms in the insurance industry, to metrics connected to firm performance. The results show cost savings and increases in ROA if the dedicated risk manager is a CRO, and even larger cost savings and increases in ROA if the dedicated risk manager is a committee instead. If the CRO reports to a committee, the CEO, or the CFO, revenues and ROA were increased.

Malik et al. (2020, p. 17) find that "effective ERM processes improve firm performance measured by Tobin's Q […]". The authors further argue that if an organization adopts effective ERM, value is created by: strategy (maximizing its market position in relation to competitors), operations (by increasing efficiency), reliable financial reporting system, and compliance with applicable law and regulations.

Al-Amri and Davydov (2016) investigate 2531 firms and conclude that ERM firms in average experience 63% reduction in operational risk frequency and on average a reduction of 35% in operational losses.

Zou et al. (2019) investigated 333 public listed firms in the manufacturing sector. The findings show, among others, that ERM firms have higher ROE compared to non-ERM firms.

Lechner and Gatzert (2018) conclude there is a negative relationship between ERM implementations and ROA. The authors argue that this could be explained by the financial and human resources that are required to implement and maintain ERM systems.

3.4.3 Knowledge Gaps of ERM Remain

Paape and Speklé (2012) find that ERM systems are more mature in publicly traded firms and organizations with a CRO and an audit committee. Conclusions from the authors are that ERM is still in a developing stage and that knowledge gaps in both practice and academe remain. Available research offers a limited amount of guidance of how effective risk management systems should be designed according to the authors.

3.4.4 Conclusions from the Articles in Group A

The articles investigate the relationship between ERM and certain financial parameters, e.g., firm value, ROA and ROE and twelve of the fourteen articles conclude that there is a positive relation between ERM and these variables. Yet, it is not concluded what the cause and effect are in these relationships.

3.5 ERM Integration with Strategy and Objectives

One aspect that authors seem to agree upon is the importance of integrating ERM with strategy and objectives. As stated in the definitions of ERM, organizations strive to achieve their objectives. These objectives are translated into a corporate strategy (Dickinson, 2001). The corporate strategy is then translated into activities, resources, and organizational structures that are needed to achieve the strategy (Dickinson, 2001). Internal factors (e.g., systems failure and production breakdown) and external factors (e.g., competitive forces and socio-political environments) impact how the outcome aligns with the corporate objectives (Dickinson, 2001). Frigo and Anderson (2011) align with Dickinson (2001) and argue that the ultimate objective of ERM is to increase the likelihood of reaching strategic objectives.

COSO (2004) argue that there is a direct relationship between corporate objectives and the ERM components. The four objective categories *strategic*, *operations*, *reporting*, and *compliance* are interconnected with the eight components of ERM (explained in section 3.6).

For ERM to create value, it must be integrated with strategy (Frigo & Anderson, 2011). Fraser and Simkins (2016); Burnaby and Hass (2009); Malik et al. (2020); Aven and Aven (2015); COSO (2004); Dickinson (2001); Lundqvist (2014) all agree that ERM should be integrated with strategy.

3.6 Components of ERM

A few articles investigate the components of ERM. Lundqvist (2014) proposes four pillars of ERM based on how organizations implement ERM dimensions: (1) *general internal environment and objective setting*, (2) *general control activities and information and communication*, (3) *holistic organization of risk management*, and (4) *specific risk identification and risk assessment activities*. The two first pillars are not directly linked to ERM activities, but all four pillars must be implemented to consider ERM as well implemented (Lundqvist, 2014). In total, the pillars contain around 50 dimensions. The dimensions in the fourth pillar are directly connected to ERM activities, e.g. consideration of strategic risk events,

but the third pillar is what Lundqvist (2014, p. 412) refers to as "truly the ERM identifier". Some of the dimensions in this pillar are a centralized unit working on risk management, determined correlations and combined effects of risks (portfolio view), formal written risk management philosophy and risk appetite, formal policies of how to manage risks, communication of risk management importance within the organization, and assigned risk owners with the main responsibility and accountability to manage risks within their areas. As the name of the third pillar suggests, the dimensions in this pillar address the holistic aspect of ERM.

COSO (2004) argues that ERM is composed of eight interrelated components:

- *Internal environment* is the foundation to how employees perceive risk and control. Philosophy and risk appetite are included here.
- *Objective setting* refers to appropriate objective setting that supports and align with the mission and risk appetite, which is ensured by ERM.
- *Event identification* refers to identification of potential events from both external and internal sources that will have an impact on reaching objectives.
- *Risk assessment* is conducted on identified risks to understand how they affect objectives and how they should be managed from both an inherent and residual point of view.
- *Risk response* include avoidance, acceptance, reduction and sharing of risks. Responses (decided by management) should align with risk appetite.
- *Control activities* include policies and procedures to ensure effective risk response management.
- *Information and communication* are necessary in all levels of an organization to identify, assess and respond to risks.
- *Monitoring* of ERM is conducted to ensure that necessary adjustments are identified and conducted.

The eight components are directly linked to *strategic*, *operations*, *reporting*, and *compliance* objectives of corporations (COSO, 2004). The eight ERM components represent what is needed to achieve the four objectives (COSO, 2004).

However, the COSO framework is not undisputed. Paape and Speklé (2012), found that applying the ERM framework by COSO (2004) did not contribute to risk management effectiveness among the organizations in their study. Their article is sorted into Group A but their finding regarding the COSO framework is presented here.

3.7 Organizational Aspects of ERM

The organizational aspects of ERM are covered in numerous articles. A selection of commonly mentioned aspects is presented in this section.

3.7.1 Top Management Involvement

Dickinson (2001) states that since ERM must be a top-down process, the CEO and senior executives must determine parameters for policies and its organizational structure for effective implementation. Burnaby and Hass (2009) emphasize the "mandate from the top", i.e., ERM must be mandated by the board of directors, CEOs and other top-level management to ensure ERM programs support in reaching organizational goals. Frigo and Anderson (2011) align with Dickinson (2001), and Burnaby and Hass (2009) that ERM is a top-down approach. Jankensgård (2019) argue that ERM should be adopted by the board of directors. Mensah and Gottwald (2016) conclude that support of top management is one of the contributors to an increase in ERM deployment.

3.7.2 Committees

The authors that cover committees in their articles are aligned on what types of committees there should be in an ERM organizational structure. The committees covered in the articles are in general two types of committees: the audit committee and the risk management committee.

Dickinson (2001) suggests that an audit committee, chaired by a non-executive director, reports to the board of directors. A committee that consists of the CEO, CFO, CRO and senior executives, decide on the strategy and enterprise risks and reports to the board of directors and the audit committee (Dickinson, 2001). Functions in the organization, e.g. production and HR, communicates risks mainly with the CRO and the CRO forwards the information to the committee (Dickinson, 2001). Brown et al. (2009) develops a risk management model for high technology firms and complex risk environments. Brown et al. (2009) argue that traditional models are not optimal for technology firms and complex risk environments since companies cannot rely on the audit committee to manage the risk management requirements. Brown et al. (2009) show that the difference between their model and traditional models is the existence of a risk management committee with members from R&D, Manufacturing, Finance, Marketing etc. The committee reports to the audit committee and the board of directors, and the audit committee reports to the board of directors (Brown et al., 2009). Fraser and Simkins (2016) is closer to Dickinson (2001) compared to Brown et al. (2009) by arguing that the management committee focusing on risk can be handled by an existing executive committee. The committee should consist of most senior executives and preferably the CEO (Fraser and Simkins, 2016).

Lundqvist (2014) includes the board-level committee with responsibility for risk management oversight, and formally defined audit committee responsibilities, in the four pillars to ERM framework. The presence of an audit committee is one of the contributors to higher level of ERM deployment according to Mensah and Gottwald (2016).

Malik et al. (2020) state that the main purpose of a board-level committee is to supervise the risk management functions and to review the process of ERM. The authors conclude that a board-level risk committee improves ERM and firm performance relationship. The authors further conclude that a board-level risk committee is crucial for ERM to be effective to the extent it increases market performance. Drew et al. (2006) suggest in their framework that a risk committee (or a CRO) should be established.

3.7.3 The CRO Role

Dedicated risk managers, or CROs as they are also called, are frequently mentioned in the articles. Dickinson (2001) argue that since identifying, controlling and managing risks across a company is complex, a dedicated specialist is required, i.e., a CRO (Dickinson, 2001). In the model by Dickinson (2001), the CRO is conducting the co-ordination and information exchange between the committee and the operational units, e.g. production, marketing, HR etc. Mensah and Gottwald (2016) find that the role of a CRO will increase ERM deployment in organizations. Fraser and Simkins (2016) frequently includes the CRO in proposed solutions for ERM implementation issues, although not explicitly stated, this can be interpreted that the CRO is considered important. Drew et al. (2006) argue that to improve leadership and its effect on risk management, boards of governors can appoint a CRO. Kimbrough and Componation (2009) concluded from their study of 2000 internal audits executives that the presence of a risk officer seemed to have a positive effect on satisfaction of ERM speed and effectiveness. The authors further found that absence of a CRO could lead to a sense of void regarding management support for ERM. From a capability-based perspective of ERM, hiring a CRO is an example of increasing risk resilience (Bogodistov & Wohlgemuth, 2017). Lundqvist (2014) emphasizes that using a CRO as an indication of ERM implementation might be misleading.

3.7.4 Centralized ERM Unit

Apart from committees and CROs, it is also suggested in the articles that there should be a centralized ERM unit in organizations. Drew et al. (2006) argue that by centralizing key risk management activities in a corporate department, leadership and its effect on risk management can be improved. Lundqvist (2014) argue that a centralized department (or staff function) that is dedicated to risk management, is one of the dimensions that enable a holistic organization of risk management. Fraser and Simkins (2016) claim that there should be a centralized group to facilitate and guide ERM. Burnaby and Hass (2009) argue that risk departments in organizations should provide information that will enable upper management and the board to compare progress with set goals, and alert of high-risk areas. Jankensgård (2019) does not claim there must be a central unit in ERM organizations but that risk exposures should be aggregated centrally in the organization. Oliva (2016) states that the degree of centralization of ERM is connected to ERM maturity where higher maturity is connected to more decentralized ERM, but mature ERM does not mean absence of central ERM units.

3.8 Risk Identification

This section covers suggestions of how risk identification can be conducted from an ERM perspective.

3.8.1 Systems-Thinking in ERM

O'Donnell (2005) presents a systems-thinking framework to identify events, which is part of ERM according to the definition by COSO (2004, p. 2). O'Donnell (2005) promotes system-thinking to understand how interdependent components together determine performance of an entire system. This logic can be applied to organizations by mapping the business model of an

organization. The business model is composed of business processes that create value for the customer, also referred to as the value chain. By creating a value chain map, the connections among the business processes are visualized. This will facilitate event identification as all interdependences are visualized and thus facilitates the understanding of how events impact business performance and in the end, the enterprise objectives.

Lee and Green (2015) promote to incorporate systems-thinking perspectives in ERM and specifically use the COSO ERM framework to show implications of systems-thinking. System-thinking could reveal synergies between components that are not present when examining the parts individually.

3.8.2 Resource-Based View of ERM

Mishra et al. (2019) argue that ERM frameworks such as COSO and ISO do not show how risks are linked to organizational resources. The authors develop a framework to show these links. The intention of the framework is to be used for risk identification and risk management. The authors categorize risks into four classes: strategic risk, operational risk, financial risk, and hazard risk. The interacting resources exposed to risks are categorized as personnel and structure, processes and plans, facilities and operational assets, customers and suppliers, and external. Key in their framework is to observe interaction sets, i.e., interactions between resources and risk classes.

3.8.3 Value Chain Focus

In line with O'Donnell (2015), Aven and Aven (2015) emphasize that risks related to activities in the value chain is what ERM should focus on. Instead of sorting risks into strategic, financial and operational risk, risks are sorted into themes based on the activities in the whole value chain to ensure completeness. Examples of these themes are access, project maturation, project execution, operation, and market. Additional themes are also added to capture specific risks, e.g., health-safety-environment, integrity, and country specific risks.

3.9 Setting Priorities in Risk Management

Setting the right priorities in risk management is covered in some of the articles and is presented in this section.

3.9.1 ERM from a Capability-Based Perspective

Bogodistov and Wohlgemuth (2017) have developed a framework for ERM based on the resource-based view and dynamic capabilities. The authors argue that the resource-based view can be utilized to help setting priorities in risk management. The resource-based view is a theory used in strategic management where the VRIN criteria can be used to achieve sustainable competitive advantage. Valuable (V), rare (R), inimitable (I), and non-substitutable (N) resources are needed for sustainable competitive advantage. These four criteria are considered by Bogodistov and Wohlgemuth (2017) to be the underlying pillars of holistic ERM. The

perspective of dynamic capabilities is incorporated in their framework as the perspective addresses how organizations can adapt their resources to cope with changing environments.

Bogodistov and Wohlgemuth (2017) suggest that resource base assessments can be conducted to identify what resources that meet the VRIN criteria. Risks related to resources that meets the VRIN criteria should be assigned highest priority. Furthermore, the authors suggest that the first-hand choice is to avoid risks. If this is not possible, mitigate or transfer the risk. If that is not possible either, accept the risk. Only if all VRIN risks are resolved, the same process can be repeated for remaining risks.

Another framework with dynamic capabilities perspective is provided by Arena et al. (2014). The authors develop a model for operationalizing ERM in project-based operations. The model is based on utilization of dynamic capabilities.

3.9.2 Hierarchy of Risk Management

Aven and Aven (2015) argue that there is a hierarchy of objectives in risk management that must be comprehended and failing to do so can lead to poor results. Risk management on lower levels in organizations can show excellent results by meeting all goals but meanwhile not contribute to the overall objectives of the organization. To ensure the correct approach is selected to support the principal objectives in the organization, distinction between Enterprise Risk Management (ERM), Task Risk Management (TRM), and Personal Risk Management (PRM) is recommended, see Figure 3.3. Furthermore, making this distinction will make communication clearer regarding risks in the enterprise.

Risk in this context is seen as deviations from reference levels, e.g., ideal states, planned values, expected values, and objectives, and associated uncertainties. Enterprise risks are deviations expressed explicitly in impact dimensions defined by the organization, usually in changes in monetary value, and in occurrence of incidents. Task risks could be delays in projects and are not expressed explicitly through the impact dimensions. Personal risks are deviations connected to compensation and/or recognition.

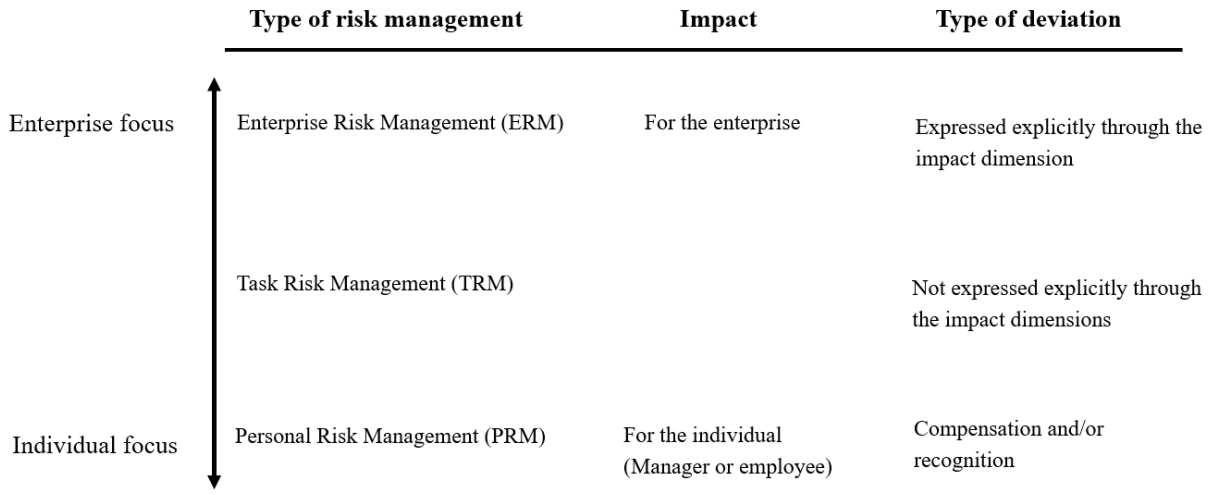


Figure 3.3. Hierarchy of risk management. Adapted from Aven and Aven (2015).

Aven and Aven (2015) argue that the hierarchy of risk management must be respected where ERM must overrule TRM and PRM to fulfill the principal objectives and exemplify how it can be problematic. A company is going to realize a project where two entities are expected to deliver on time, and at the right cost and quality. Risk assessments in one entity indicate high probability for a three-month delay. Management of the entity considers to either increase manpower to meet deadline, or to focus on critical lines and avoid further delays. The goals for the entity management are already decided and a compensation scheme is attached to it. The incentives for management to increase manpower is thus strong, despite higher costs. TRM and PRM are highly influencing management when they decide to increase manpower. However, it later turns out that the delivery of the other entity is delayed by more than three months. From an ERM perspective it does not make sense to invest in manpower if the organization will not manage the deadline anyway. But from a TRM and PRM perspective at the entity level, the choice was right given the available information and circumstances. It is essential that risk and uncertainty reduction measures must be in relation to ERM objectives.

3.9.3 Suboptimal Risk Management

The increase in manpower in the example by Aven and Aven (2015) is an example of suboptimal risk management. The authors further argue that successful ERM can avoid suboptimal risk management by making sure that incentives can run in parallel. Single entities cannot optimize on behalf of the entire organization. Successful ERM requires that information flows from entities to the asset owners that conduct ERM. Another measure to prevent suboptimal risk management is to make sure risk management is focused on principal objectives of an organization and not focus on increasing KPIs, which is sometimes the case (Aven & Aven, 2015)

Jankensgård (2019) proposes that ERM is viewed as a solution, adopted by the board of directors, to solve two types of problems of risk management: the *agency problem* and *information problem.* Suboptimal risk management occur because silos (corporate functions and operating units) are run by agents that over-manage or under-manage certain categories of risks depending on their incentives and biases (agency problem). The agency problem of risk management occurs when agents and principals disagree on the amount of residual risk to be absorbed by the firm. Over-management of risks occurs when agents overspend resources on measures to mitigate risks. The cost of mitigating such risks is considered higher than the benefits of the mitigation. Under-management of risks occurs when principals desire risk mitigation measures, but agents are not undertaking these measures.

Jankensgård (2019) argue that the category of risks that are likely to be under-managed are high impact - low probability risks. Under-management of risks is generally due to individual behavioural biases and/or distorted incentives. Three types of behavioural biases are oversimplification, over-optimism, and overconfidence where a combination of the three create under-management of risks. Over-management of risks tends to occur for high probability – high salience risks. These risks are easily observed and considered as important and likely to occur. The compensation of the agent can also be directly linked to these risks through metrics. Currency risk is one such example since it has evident links to financial performance and is known to fluctuate. KPIs can also contribute to that risk exposure become salient. Furthermore,

Jankensgård (2019) refers to Lynch (2008) arguing that recent failures and events tend to become salient as excessive focus is aimed at prevention of reoccurrence.

3.10 Risk Aggregation

Literature on risk aggregation is limited in the scoping study. Risk aggregation is mentioned by Tekathen and Dechow (2013) that include risk aggregation practices as one of seven themes that is considered to contribute to enterprise-wide risk management. The themes are used in their study to structure data, but risk aggregation is not of focus in their study and is not discussed further. Jankensgård (2019) is the only author who elaborates on risk aggregation among the authors in the scoping study. Jankensgård (2019, p. 575) defines risk aggregation as

"[…] a set of mechanisms used to ensure that high-quality information about risk is aggregated in a timely, intelligible and relevant format to support centralized decision-making regarding the deployment of economic capital".

Jankensgård (2019) claims that current ERM programs have limited contribution to discussions on aggregated risks of organizations.

3.10.1 Risk Aggregation as a Solution to the Information Problem in ERM

As discussed earlier, Jankensgård (2019) claim that ERM seeks to solve the agency problem and information problems of risk management. The information problem is a result of the decentralized decision-making structure of agents operating in silos where the information that reaches the board is insufficient to properly assess the organization's overall risk profile. The information presented to the board does not contain risk exposure and risk mitigation actions undertaken in the silos, hence measures are implemented to aggregate information about net risk exposures centrally in the organization. The aggregation of risks allows the board to utilize capital to support the risk level in the portfolio of risks. This is conducted with consideration to interdependencies between risks in the operating units. Additional benefits of aggregating risk information centrally include co-ordination of risk mitigation activities and external communication of risk management.

3.10.2 Presenting Risk Information to Facilitate Risk Aggregation

Jankensgård (2019) argues that risk exposures must be available, of sufficient quality, standardized and presented quantitatively to enable comparisons. Probability and impact dimensions of each risk is commonly adopted to quantify risks where impact is usually expressed in currency. This information must be reported to upper management through a reporting process. However, it is important that upper management is not overloaded with information. Jankensgård (2019) points out that compilations of risks can be useful to discuss, e.g., mitigation actions, but is insufficient to show how interdependences between risks impact the overall risk level.

3.11 Conclusions from the Scoping Study

Twelve of the fourteen articles in Group A concluded that ERM have a positive relationship with certain financial indicators. However, the cause-effect relationship is not clarified.

The literature in Group B and Group C highlights why certain aspects of ERM are important but do not provide much guidance on how to conduct successful ERM. For example, it is stated that ERM should be integrated with strategy and objectives but there is not much guidance on how ERM is integrated with strategy and objectives or how to determine if ERM is integrated with strategy and objectives.

Furthermore, literature in all groups covers risk aggregation to a limited extent. Synonyms to risk aggregation, e.g. risk consolidation or similar was not covered either. The lacking literature on risk aggregation in the scoping study indicates a gap on risk aggregation in ERM literature in general. It is assumed that risk aggregation must be conducted for ERM to be successful since large numbers of risks is difficult, perhaps even impossible, for a board of directors to evaluate. The decision was made to find more literature on risk aggregation, but outside the ERM context, which is presented in the next chapter.

4 Additional Literature

This chapter contains additional literature on risk aggregation which was not included in the scoping study. The content in this chapter is obtained by using backward snowballing in the scoping study articles. The importance of risk aggregation is further highlighted by Alviniussen and Jankensgård (2009) claiming that corporate risk management cannot be classified as ERM unless risks are aggregated and managed centrally.

4.1 Model for Aggregation of Risk Information

Hassel (2018) presents a framework intended for aggregation of risk and vulnerabilities assessments (RVA) in Swedish municipalities, illustrated in Figure 4.1. Although there are some differences in the context, it is believed that the framework is applicable in ERM contexts as well.

The components in the framework for aggregating risk information proposed by Hassel (2018) include *risk information* and *support needs* which must be transferred from sub-system level to system level, and that *instructions and procedures*, *information/knowledge basis*, and *support and guidance* are transferred from the system level down to the sub-system level. Three of the six components are necessary for a risk aggregation process: instructions and procedures, risk information, and the aggregation mechanism. The remaining three components can be added to ensure high quality of the RVA processes, both in sub-system level and system level.

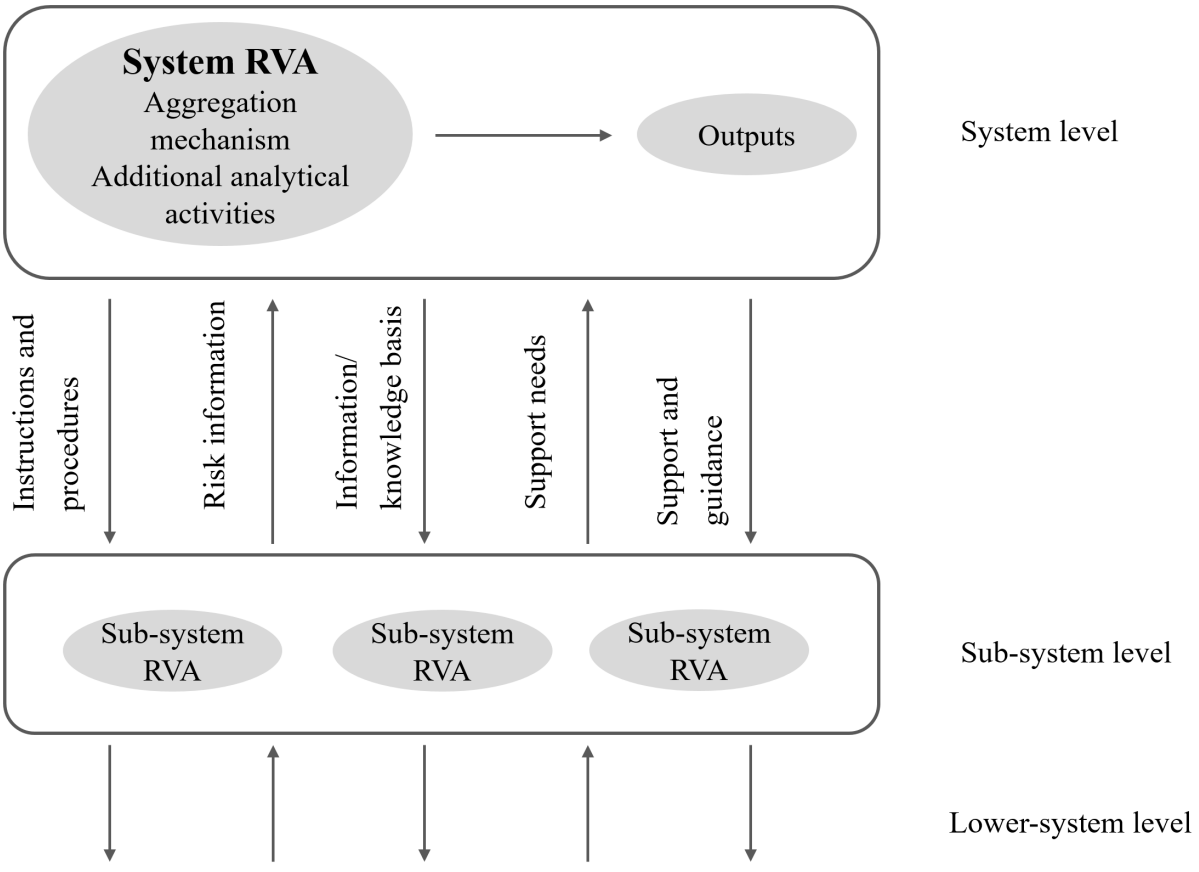


Figure 4.1. Model for aggregation of risk information. Adapted from Hassel (2018).

Instructions and procedures have the purpose to facilitate aggregation (of risk information) by harmonization of the risk information, e.g. by ensuring that scales of different RVA are compatible.

The *risk information* should be presented to the system level in accordance with the instructions and procedures. Hassel (2018) emphasizes information security when risk information is sent from external actors on sub-system levels to the system level.

Furthermore, there must also be an *aggregation mechanism* on the system level to produce the desired outcome on a system level. Risk information is collected, stored, and processed from the sub-system levels and additional analytical activities may also be needed to aggregate the risk information.

Information and knowledge bases should be provided to the sub-system levels by the system level. This refers to information that the sub-system levels need but may require resources to collect. It is more efficient if the system-level collects the information and provide it to the sub-system levels. Preferably, the information concerns aspects that are not varying in the sub-system levels, e.g. likelihood of external events.

Support needs and guidance is aiming to develop the quality of the RVA. If sub-system level needs support, it should be communicated to the system level. The system-level is then expected to provide guidance to the sub-system levels. If sub-systems are facing issues, it is more efficient that the system-level solves these issues instead of each unit in isolation. Improving quality is important as it could improve aggregation on the system-level.

4.2 Uncommon Categorization in Risk Information

Månsson et al. (2015) investigate the presence and effects of uncommon categorizations in disaster risk management systems. Uncommon categorization refers to differences in how similar terms and information are interpreted, coded, and categorized. High levels of uncommon categorization in combination with relatively low precision and lack of background information, make it difficult to synthesize information from different stakeholders. Lack of commonality in: (1*) assessments of likelihood, consequence, and capabilities in risk and vulnerability assessments* (2) *Nomenclature*, and (3) *methodology of how stakeholders analyse and present risk information,* are causes of uncommon categorization. Table 4.1 shows examples of what challenges lacking commonality in these areas could lead to.

Table 4.1. Challenges from lacking commonality in different areas.

Lack of commonality in	Example of challenges
Assessments of likelihood, consequence, and capabilities in RVAs	How does one assess "Good capability" or "fairly good capability"?
Nomenclature	If fundamental terms like risk, capability and vulnerability are not defined, it can lead to various interpretations.
Methodology of how stakeholders analyse and present risk information	Interpretation is required if amount, type, or format of requested information is not specified. What level of detail is requested? Should risk matrices be used?

An activity to partly reduce the uncommon categorization is workshops as they increase probability of detecting interdependencies between stakeholders and facilitate alignment of stakeholders regarding interpretations of scenarios and scales for assess risk and vulnerability (Månsson et al., 2015).

Additional causes of uncommon categorization are lack of time for feedback and fully understanding information, and the mixed purposes of RVAs. In the study by Månsson et al. (2015), one purpose of the RVA is to provide an assessment for the organization in question, and the other to provide information as input to determine a collective risk profile for (in this case) the whole of society. The authors concluded that focusing on one of the purposes undermined the possiblity of accomplishing the other.

4.3 Presenting Risk Information to Facilitate Risk Aggregation

Månsson et al. (2015) highlight that scales with common reference points enhances comparisons between assessments. Such scales include semi-quantitative ordinal scales and quantitative scales. Another important aspect is that differences in how multiple risks are described will influence their consolidated usefulness for decision making and for risk levels comparisons (Månsson et al., 2019). The impact of mixing risk descriptions is especially negative when comparing risk levels in different parts of a larger system where single assessments alone do not cover the scope (Månsson et al., 2019). Such examples are geographical areas, functional sectors, or a large company.

Regarding the use of qualitative and quantitative estimates in risk assessments, quantitative elements is, in general, preferred if they are used as a basis for risk reduction measures (Månsson et al., 2019). However, it is unknown whether *advanced* quantitative elements are preferred over qualitative. Månsson et al. (2019) refer to previous studies showing that complex quantitative elements might have negative effects as they rely on numerical abilities of the recipients. One of these studies is made by Peters (2008) who highlights the discrepancies between highly numerate individuals and less numerate individuals in terms of: paying attention to numbers associated with risk, understanding them, translating them into meaningful information, and to use them in decisions. Peters (2008) emphasizes that if attention is aimed

at how information is presented, to target both highly numerate and less numerate individuals, risk communication efforts across diverse stakeholder groups are likely improved.

4.4 The Importance of Background Knowledge in Risk Aggregation

Lack of background information contributes to difficulties in synthesizing information (Månsson et al., 2015). Providing background knowledge that motivates risk assessments support how qualitative elements (likely, severe etc.) should be interpreted (Månsson et al., 2019). Additionally, providing background knowledge facilitates merging of risk descriptions containing different scales, i.e., qualitative, semi-qualitative, and quantitative (Månsson et al., 2019). This in turn will increase the probability of aggregating information from several stakeholders with varying ways of presenting risks (Månsson et al., 2019). Background knowledge can be increased by having workshops to enable discussions between stakeholders (Månsson et al., 2015). Bjørnsen and Aven (2019) stress that when risks characterizations are aggregated, not only should background knowledge of each isoloated risk be provided, but also the background knowledge of the risks in combination, i.e. when the risks are aggregated.

5 Case Study

This chapter aims to answer RQ2. The emphasis is on risk aggregation. The data presented in this chapter was collected from a combination of interviews, a risk consolidation workshop, meetings, and documentation from the case company.

5.1 Case Company Introduction

The information about the case company is limited since the case company is anonymous. The case company manufactures high technology products and has manufacturing plants and offices in multiple countries (Sweden among others) and with sales worldwide. The company faces a variety of risks, e.g., risks related to supply chains, cyber security, and manufacturing. Considering the vast amount of risks the company manages, it is an interesting company to analyse from an ERM perspective.

5.2 Organizational Structure

The organizational structure logic of the company is illustrated in Figure 5.1 and is based on organizational charts that were provided by the company. Observe that the purpose is to illustrate the logic of the organizational structure and not to show the entire structure of the company. The exact structure is not presented due to practical reasons as the company contains around 10-15 functions and several managers under each head of function.

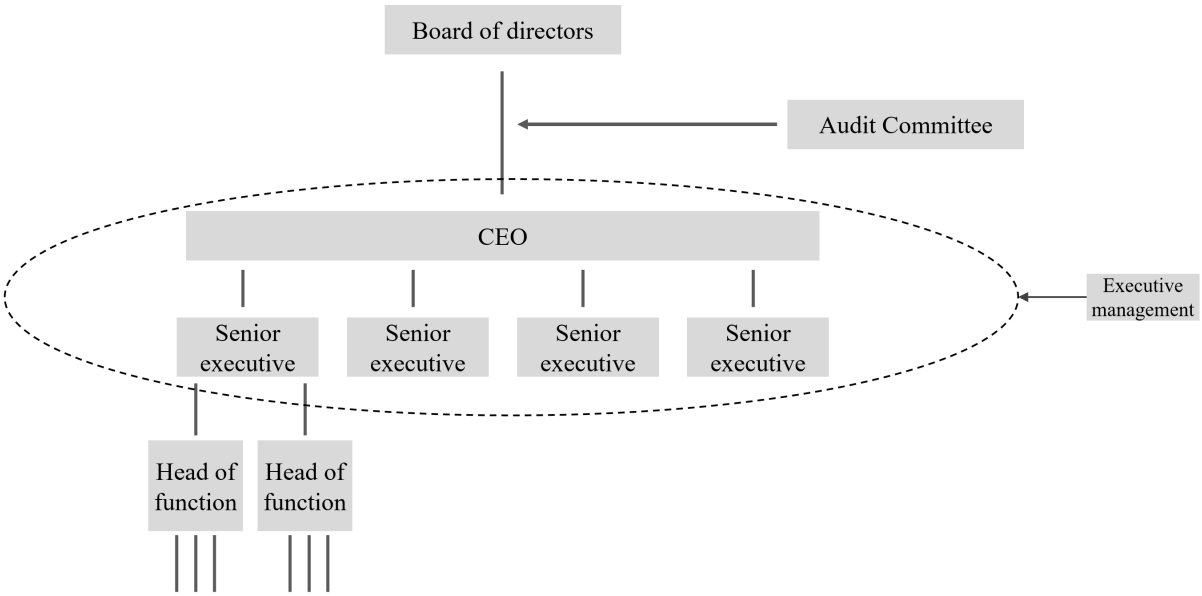


Figure 5.1. Organizational structure of the company.

The CEO and senior executives constitute Executive Management (EM). EM reports to the board of directors and is audited by the audit committee. The audit committee is a subset of the board with focus on financial reporting related topics. Within each function, head of functions are reporting to the senior executives. The senior executives have different numbers of head of functions reporting to them. The ERM team is located further down in the hierarchy in one of the functions.

5.3 ERM Organizational Structure

It was concluded in the scoping study that several articles covered organizational aspects of ERM, especially CRO, audit committees, and risk committees. Due to this, the same organizational aspects of ERM were investigated at the company. The descriptions of functional risk managers, risk area owners, the risk committee, ERM team, and ERM core team were found in role descriptions. The description of the audit committee and the board of directors were found in procedural documentation for risk management.

Risk Owner
The individual or entity with the accountability and authority to manage a risk.

Functional Risk Managers
The functional risk managers work with risk management in specific functions, e.g., cyber security, procurement, sustainability, quality, and HR. There are approximately 15 functional risk managers in total.

Risk Area Owners
Risk area owners are the subject matter experts of risks. The risk area owners drive progress of the risk monitoring. Some of the risk area owners are also functional risk managers. Most of the risk owners are managers. There are approximately 25 risk area owners.

Compliance Roles
Roles responsible for internal control in their function.

Risk Committee
The risk committee (RC) consists of around 30 members. The members are functional risk managers, risk area owners, and compliance roles, see Figure 5.2.

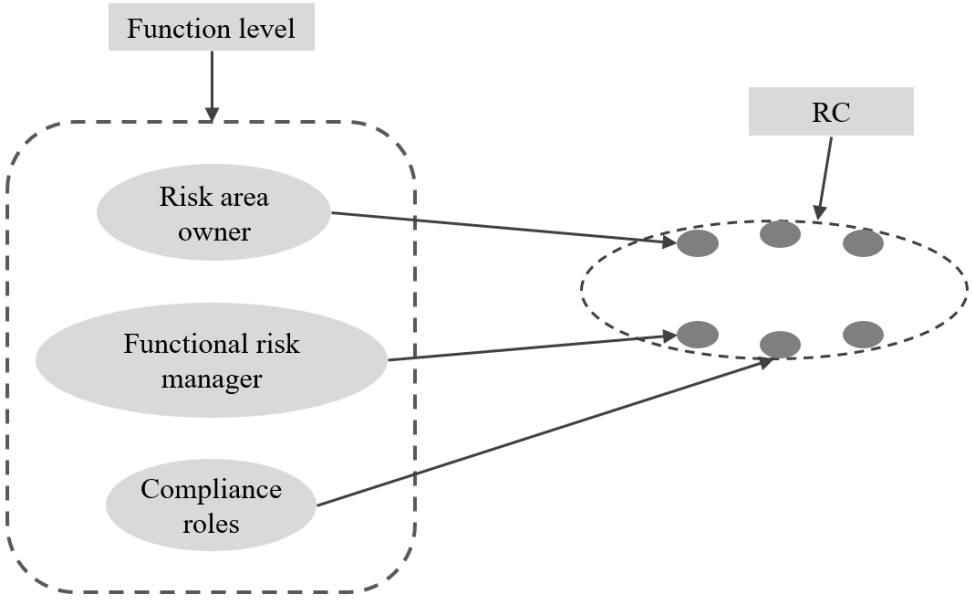


Figure 5.2. Members of the Risk Committee (RC).

RC is open for everyone in the company working with risks or find risks interesting, hence there is a variety of roles. RC is fundamental for conducting ERM since there is no organization in place dedicated for only ERM, except for the ERM team. Instead, ERM relies on networking between its members and the ERM team.

ERM Team
The ERM team is led by the risk management officer and is responsible to drive ERM activities and the ERM reporting process.

ERM Core Team
Members of the ERM core team are, in general, head of functions that report to the senior executives. The prerequisite for the members is not to be head of functions but to have a strategic knowledge of their function and the company to make the right decisions. However, the people who have strategic understanding of their functions often have the role as head of function. Furthermore, it is important that the members represent as many functions as possible to mirror the company. The size of the ERM core team is approximately half the size of RC. Most of the members in the ERM core team are *not* members in RC.

Audit Committee and Board of Directors
Board of directors sets the risk management procedures and risk appetite for the company and regularly review risk areas and monitors and contributes to internal strategies and activities for risk treatment. The audit committee has the delegated responsibility from the board to perform these reviews.

5.4 ERM Reporting Process

The ERM reporting process in the company refers to how risks are communicated from functions up to EM and subsequently to Board of directors. The information of how the ERM reporting process is conducted was obtained by observations from participation in a full-day consolidation workshop and RC meetings. Continuous dialogue and meetings with the ERM team was subsequently used to assure information is correct.

Figure 5.3 illustrates the ERM reporting process which is conducted twice per year. The ERM reporting process focuses on functions. Functional risk managers collect information in their function about identified risks, estimated risk gradings, and background information. The information is sent in excel sheets (implementation of a software is ongoing where risks can be reported into a system instead) to the ERM team. When all functions have reported, the ERM team starts reviewing all risks. Risks are sorted into categories and levels, and risk scores are calculated based on provided gradings. The risks are subsequently inserted into a heat map. Risks are evaluated against strategies and other objectives and targets.

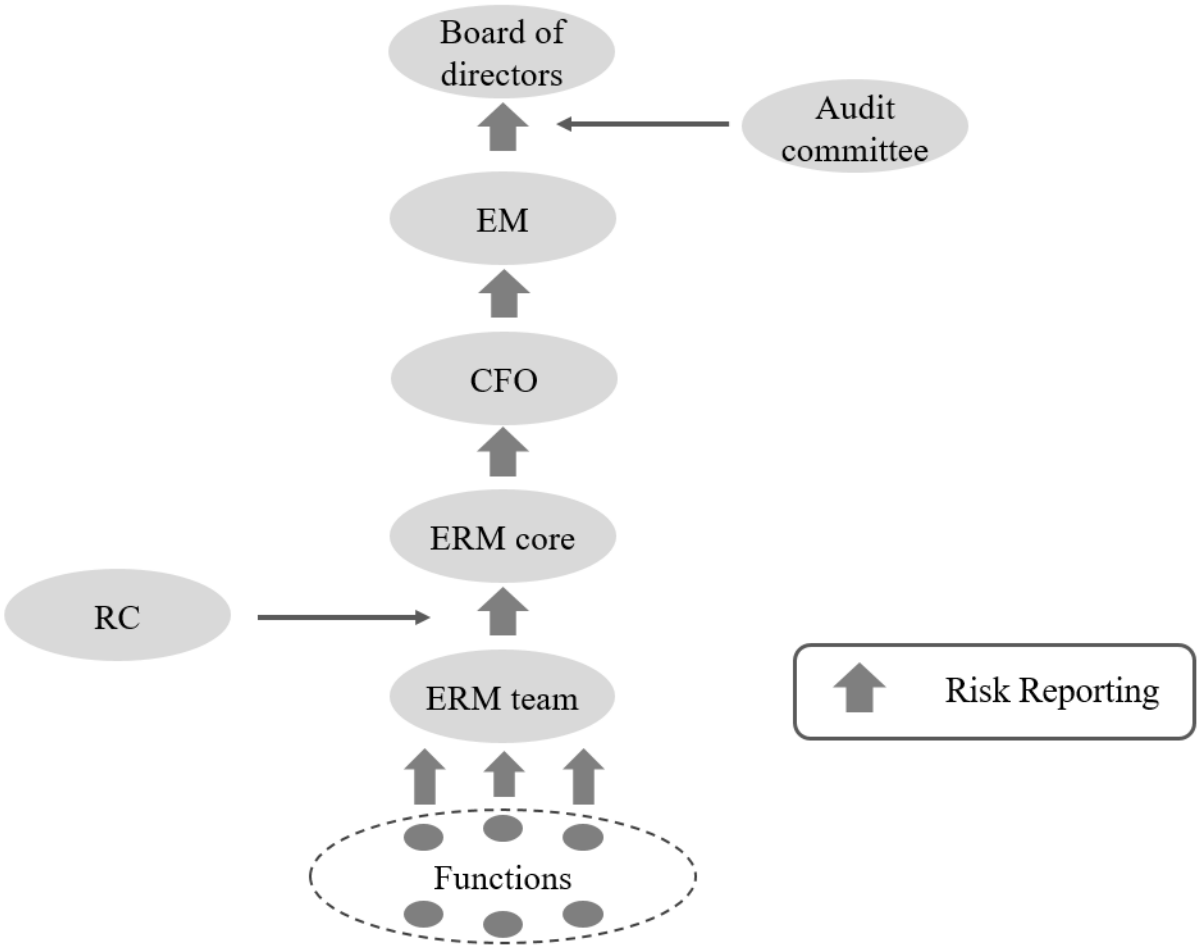


Figure 5.3. Risk reporting in the ERM reporting process.

The ERM team have continuous contact with functions during the ERM reporting process to ensure that functions are aligned regarding the risks. RC serves as a forum for alignment, information sharing, and discussions in the ERM reporting process. When the ERM team has reviewed all reported risks, the risks are presented to ERM core team.

Two meetings are held with the ERM core team where voting of what risks to prioritize and thus forward to EM is conducted in the second meeting. Correct representation of members in the ERM core is essential to ensure that members reflect the company. Outcome from the voting is not binding as the risk management officer (in ERM team) makes the final decision. In the next step of the ERM reporting process, the CFO is informed of what will be presented to EM. Subsequently, EM reviews the list of risks and suggest adjustments, e.g., to aggregate risks or remove risks that are considered as not prioritized. When adjustments are finalized, the reported risks are presented to the Audit Committee and filed with the board.

5.5 Risk Categorization

During participation in the consolidation workshop, it was observed that after functions have reported risks, ERM team categorize the risks. Each risk is categorized into one of four areas:

- Strategic – Risks that may impact strategic objectives
- Operational – Risks that may interfere with operations
- Compliance – Risks that may impact compliance with laws and regulations
- Financial – Risks that may impact the financial result and/or valuation

One type of category is not prioritized over another. The categories are utilized to ensure that different types of risks are captured in the reporting process.

5.6 Evaluation of Risks Against Corporate Strategies and Business Plan

The four risk categories above are utilized to evaluate risks against corporate strategies. Figure 5.4 shows how the top 20 risks (selected by voting in ERM core) are evaluated against corporate strategies. Potential opportunities are also considered. The risks and strategies A, B, and C in Figure 5.4 are undisclosed for confidential reasons.

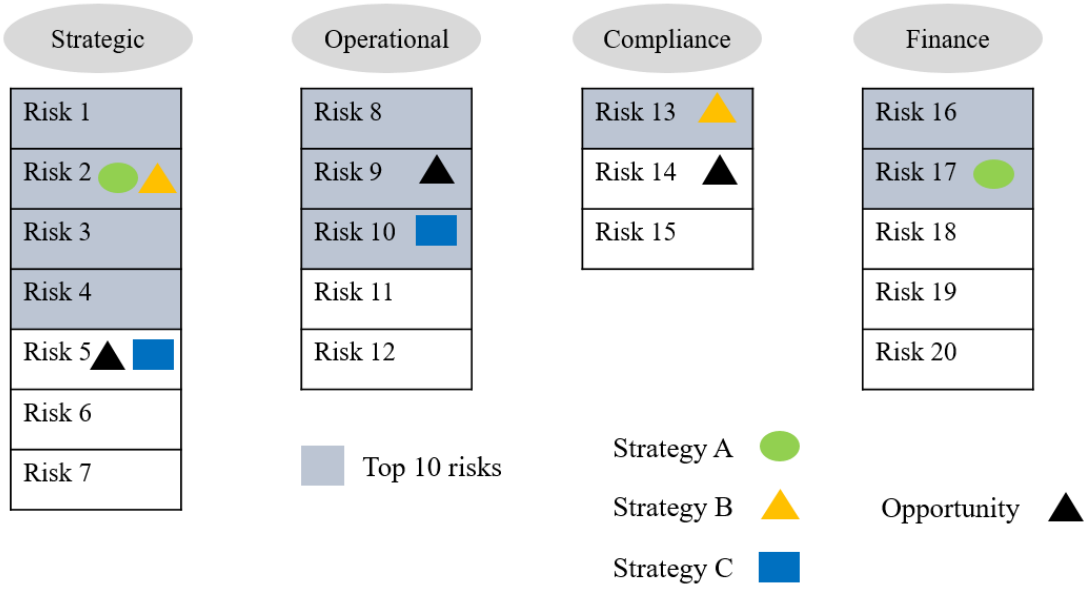


Figure 5.4. How risks are evaluated against corporate strategies.

A selection of the top 20 risks is further evaluated against the current business plan. The risks estimated to have considerable financial impact are evaluated within the business plan. Impact of the selected risks on certain parameters, e.g. EBIT, are calculated and compared to the business plan. Background information, e.g. geopolitical factors, is collected regarding the risks to estimate impact. From the selected risks (of the 20 top risks), a few is selected and aggregated to create a scenario that considers several risks in combination and how it would affect the business plan.

5.7 Risk Aggregation Levels

During the consolidation workshop it was observed that risks are sorted into aggregation levels. Level one is an aggregation of the risks in level two, which is an aggregation of the risks in level three and so on. There is no official limitation in number of levels as functions decide themselves how risk management should be conducted in their function. However, the first four levels are the most occurring ones in the ERM reporting process:

- Level 1 – Risk areas
- Level 2 – ERM risks
- Level 3 – Functional key risks
- Level 4 – Functional detailed risks

What determines the level is the potential impact of the risk. Level two risks are considered to impact several functions in the company. Level three risks are considered to have impact on an entire function. Level four risks are estimated to impact limited parts of functions and are not reported to the ERM team. The risk areas (level one risks) are mainly utilized for visual purposes and is useful in workshops etc. There are currently 30 risk areas e.g., sustainability & environmental, and material cost & supply chain. The aggregation levels are used with flexibility as there are additional aspects that must be considered.

The intention is that risks reported by functions to the ERM team are level two or level three risks. Preferably, functions have either aggregated level four risks into level three risks or identified single risks that are considered as level three risks. However, as functions decide much of risk management themselves, it is not a requirement to work with aggregation levels and hence there are risks reported that are not evaluated regarding aggregation levels. Figure 5.5 shows an example of how aggregation levels are applied. Figure 5.5 is adapted from parts of a tree structure created by the ERM team.

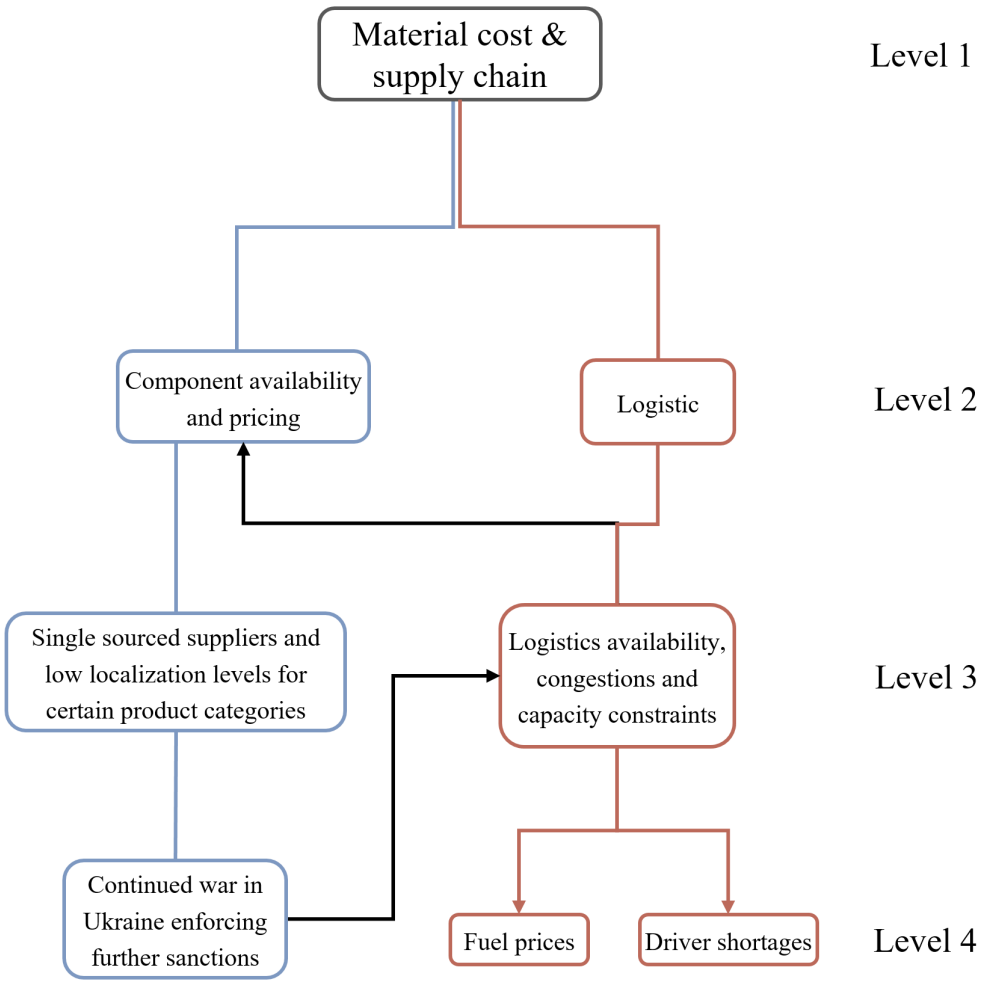


Figure 5.5. Example how the risk aggregation levels are used in a tree structure.

The level one risk is one of the 30 risk areas. The three levels below it shows how risks can be aggregated using the aggregation levels.

Risk Aggregation in Numbers

The approximated number of risks (estimated by the ERM team) in each stage in the ERM reporting process is illustrated to the left in Figure 5.6. Starting from the bottom in Figure 5.6, the number of identified risks in total for all the functions is unknown. Risk aggregation could also be conducted inside the functions.

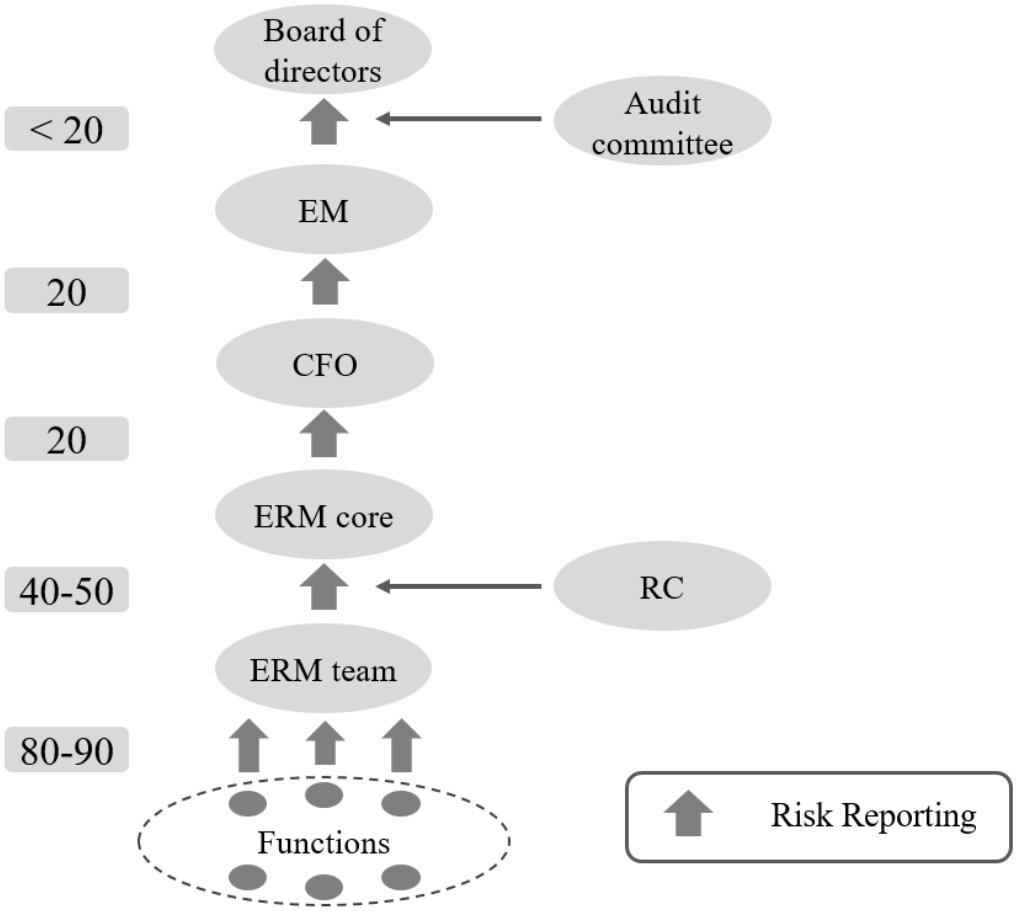


Figure 5.6. The approximate number of risks in the ERM reporting process.

In the next step, the ERM team aggregate the approximately 80-90 risks (level two and level three risks) reported, into around 40-50 risks which are subsequently discussed in the ERM core team meeting. The list of risks after voting in ERM core team meeting contains 20 risks. The 20 risks are often reduced during EM reviewal as risks are aggregated and removed if they should be down prioritized. Furthermore, risks that are considered important but not on the list can be added by EM.

5.8 Risk Information

Documentation was provided that contained the guidelines for risk information. The risks that are reported to the ERM team must contain certain information. The guidelines issued by the ERM team states that risk information should contain seven different types of information:

- Risk description
- Risk outlook
- Risk owner
- Risk drivers and monitoring
- Risk evaluation
- Risk response
- Risk acceptance

The seven types of information are explained in detail in Appendix B.

Observations of Risk Information

It was observed during the consolidation workshop that some risks did not contain risk information and other risks contained detailed information. Some risks contained all impact dimensions and gradings but no background information which made the dimensions difficult to interpret.

5.9 Risk Reporting Process in a Function

An interview was conducted with a functional risk manager in one of the functions to understand the risk reporting process in a function and up to the ERM team. The process and the approximate number of risks is illustrated in Figure 5.7.

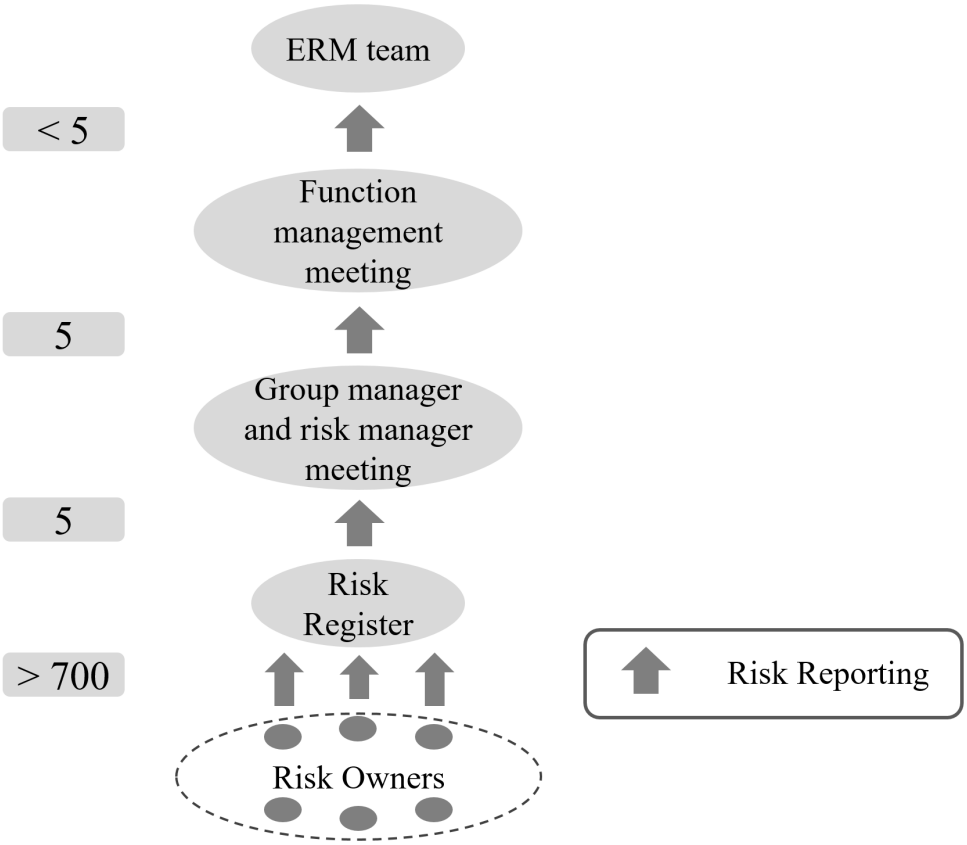


Figure 5.7. Risk reporting in one of the functions and approximate number of risks.

The function has a risk register which risk owners are responsible to keep updated. The risk manager and group manager have regular meetings to align on what risks that should be discussed in the function management meeting where decision is made on what risks to forward the ERM team. The risk register contains more than 700 risks at the time of the interview. The risk manager creates approximately five risks based on the risks in the risk register. The word "creates" is used as risks are never picked directly from the risk register and all 700 risks are not aggregated into the five risks. The five risks are created based on aggregation and a selection of risks to prioritize. The risk score is central in selection of what risks to prioritize.

It is required to estimate impact and likelihood when risks are added in the risk register. A risk matrix is used for this purpose where the x-axis is financial impact (expressed in SEK) and the y-axis is likelihood (expressed in frequency). Both axes are divided into eight intervals with

corresponding SEK and frequency assigned to them. The intervals are used to calculate a risk score, e.g. if financial impact is interval 6 and likelihood interval 4, it yields a score of 6*4 = 24.

The risk manager subsequently discusses the five risks with the group manager. Often the same risks are forwarded to the function management meeting where higher managers in the function align on what risks that should be forwarded to the ERM team. A few of the five risks are removed, often because management of the function thinks financial impact is exaggerated.

Risk Aggregation in the Function

In the function, the risk manager aggregates risks if needed. The risk manager emphasizes the importance of not simply adding risks. Risks must be evaluated individually to determine if they are possible to combine. The risk manager explains that aggregation of risks could be suitable when impact area or vulnerability is the same, and when risks are too detailed. Risks that are too detailed may not necessarily be aggregated with another risk, but are transformed into higher aggregation levels, which enables future risks to be aggregated with them. Situations unsuitable for risk aggregation could be if risks have different risk owners, as it will be unclear who the risk owner is. Both technical and process solutions could be added into the risks which makes it more difficult to execute solutions if risks are aggregated.

6 Analysis

This chapter aims to answer RQ3 and is divided into two parts. The findings from the case company are analysed and compared to the literature in the first part. In the second part, improvements suggestions are provided based on the first part.

6.1 Case Company Analysis

The selection of what to study in this section is based on the findings in the literature and in the case company. ERM integration with strategy and objectives, and organizational aspects of ERM are analysed as they are emphasized in ERM literature. Risk information is analysed as it is central in risk aggregation literature. The ERM reporting process in the company is examined since it is connected to risk aggregation.

6.1.1 ERM Integration with Strategy and Objectives

As described in section 3.5, multiple authors agree that ERM should be integrated with strategy and objectives. The purpose of ERM integration with strategy and objectives is provided in the literature but not how to determine if ERM is integrated with strategy and objectives. This section analyses the collected information in an attempt to conclude if ERM is integrated with strategy and objectives in the case company.

Risk Area Categorization

The first sign of ERM integration with strategy and objectives is that risks are categorized and evaluated based on the four areas described in section 5.5. Three of the four risk areas are the same as the objectives of COSO (2004) as seen in Table 6.1.

Table 6.1. Comparison of COSO (2004) objective categories and risk area categorization conducted at the case company.

COSO (2004) objective categories	Case company risk area categorization
Strategic	Strategic
Operations	Operational
Compliance	Compliance
Reporting	Financial

COSO (2004) argues that the objective categories represent what the company aims to achieve and the ERM components represent what is required to achieve them. The ERM components are directly linked to the objectives categories according to COSO (2004). Since the case company evaluates risks in reference to these four categories that are almost the same as the COSO objectives, it is an indication that ERM is integrated with strategy and objectives in the company.

Risk Evaluation Against Corporate Strategies and Business Plan
All risks are in essence derived from reviews of corporate strategies and objectives as each function evaluates risks against their strategies and objectives. When risks are reported to the ERM team in the ERM reporting process, risks are sorted into the four objective categories in Table 6.1. Later in the ERM reporting process, the ERM core team makes further prioritization based on strategies and objectives. These activities show that ERM is integrated with strategy and objectives. The selection of risks (among the top 20 risks) that are evaluated within the business plan due to their estimated financial impact, and which later may be used to create scenarios to investigate the impact on the business plan, further shows that ERM is integrated with strategy and objectives.

Impact Evaluation of Risks
All the six impact areas (Figure B.1 in Appendix B) that are used for impact evaluation are developed based on strategies and policies. Evaluating impact against areas that are connected to strategies and objectives of the case company further suggest ERM is integrated into strategies and objectives.

ERM Core Review
Another sign of ERM integration with strategy and objectives is found in the ERM core review. The prerequisite that members have strategic understanding of functions indicates that the company integrates ERM into the strategy and objectives of the company. Strategic understanding is important to understand potential impact on functions.

6.1.2 Organizational Aspects of ERM

Described organizational aspects of ERM in the literature were top management involvement, committees, role of the CRO, centralized ERM unit, and assigned risk owners.

Top Management Involvement
The literature concludes that ERM should be mandated from top management/board of directors which aligns with the case company where ERM team reports to EM. Dickinson (2001) suggests that CEO and senior executives determine parameters for policies in ERM. Regarding policies for ERM in the case company, the board of directors and the audit committee set the risk management procedures and risk appetite and contribute to internal strategies and activities for risk management. CEO is part of EM and thus involved in the ERM reporting process.

CRO
The formal title CRO does not exist in the case company but the risk management officer in the ERM team has similar responsibilities of a CRO by being responsible and accountable for the ERM in the company. However, the risk management officer in the case company is on a lower hierarchical position compared to what a CRO would be as described in the literature. This could impact ERM in different ways, e.g. in decision-making since there is no representative from risk management in EM.

Committees

Dickinson (2001) suggests that a committee containing the CEO, CFO, CRO and senior executives, should decide on enterprise risks and strategy and that communication of risks from the functions to the committee is conducted via the CRO. The suggested committee is similar to EM in the case company but there are differences. There is no dedicated CRO, instead there is a risk management officer (not C-level executive), and communication from the functions of risks to EM is not conducted only by the risk management officer. Instead, head of functions are responsible to communicate risks to EM.

The risk management committee suggested by Brown et al. (2009) with representatives from functions is similar to RC in the case company. The authors claim that their model is suitable for high technology firms in complex risk environments, which aligns with the case company working with high technology. The audit committee in the case company is involved in ERM as described earlier, e.g., in risk management procedures and setting risk appetite.

Centralized ERM Unit

Several of the authors argue that there should be a central ERM unit in organizations that is dedicated to ERM. In the case company, this is the ERM team. In line with Lundqvist (2014) stating that the central unit is important to enable a holistic organization in risk management, it is observed in the case company that ERM team is the enabler for this. Conducted activities includes organizing all ERM activities, guidance and training on ERM, development of tools, risk aggregation and more.

Audit Committee and Board of Directors

As limited information was obtained regarding ERM in the audit committee and the board of directors, they are excluded from the analysis.

Risk Owners and Risk Area Owners

The case company assigns risk area owners and risk owners. This is in line with Lundqvist (2014), including allocation of risk owners who are responsible and accountable for risks in their areas, in the third pillar of ERM.

6.1.3 The ERM Reporting Process

The ERM reporting process in the case company is analysed in this section.

Selection of what Risks to Prioritize

In the ERM reporting process it was discovered that selecting what risks to prioritize, in addition to risk aggregation, is utilized to transform large number of risks into manageable amounts and to illustrate the total risk exposure of the company. Risk scores are used to facilitate what risks should be selected and hence prioritized. Preferably, only aggregation should be used to avoid biases when risks are selected, but it is in practice difficult. Selecting what risks to prioritize could be problematic, e.g. if five risks out of 100 are selected based on their risk scores and subsequently are aggregated, the five risks will not necessarily represent total risk exposure. However, completely eliminating selection is not realistic as only using aggregation at all levels would be difficult and create new problems, e.g., if five risks with five different risk owners are aggregated into a single risk, who is the risk owner? Shared responsibility between five people is likely not successful. Risk selection could thus remain in the ERM reporting process but can be improved.

Awareness of Over- and Under Management of Risks

Raising awareness of over- and under management of risks described by Jankensgård (2019) is important, especially in situations of risk selection. Under-management is generally due to behavioural biases and/or distorted incentives and usually affects high impact – low probability risks, which would translate to the second highest grading (ERM awareness). Hence, these types of risks are intended to get attention of EM but are also the risks that are most likely to be under-managed. Risks that tend to be over-managed should be observed as costs of mitigation activities may not be in line with risk appetite.

Difficulties in Estimating Impact from an ERM Perspective at Function Level

According to the interviewed functional risk manager, individuals, e.g. technicians or risk owners in that function, are assigning likelihood and impact to risks which yields a risk score. The score is subsequently used as support for the risk manager to select what risks that should be discussed with management in the function and later be reported to the ERM team in the ERM reporting process. It is however difficult for risk owners and technicians to estimate impact in relation to ERM objectives as they have limited company-level information and it may not even be preferred that they attempt to estimate impact in relation to ERM objectives. As impact is in relation to objectives, it is important as Aven and Aven (2015) argue that objectives in the hierarchy of risk management align to avoid conflicts.

The example with the project delay by Aven and Aven (2015) in section 3.9.2 shows that a risk can have higher impact in relation to the objectives of the function, compared to in relation to objectives of the company. Personal risk management as Aven and Aven (2015) describe may also influence impact estimation, e.g. impact in relation to objectives of a specific employee creates incentives for that employee to assign high impact to the risk. Managers play a crucial role in translating the impact of a specific risk into what it may mean for the entire function and perhaps also for the company. Managers are more suitable to make these judgements as they are expected to be aware of the objectives. It is unknown whether the various functions in the

case company involves managers in such decisions, but at least it is the case for one function (function of the interviewed risk manager) and for the ERM process on a company level.

6.1.4 Risk Aggregation

The framework for risk aggregation by Hassel (2018) in section 4.1 is compared to the case company in this section. The functions in the case company are seen as the sub-system level and the ERM team is seen as the system-level in the framework by Hassel (2018).

Instructions and Procedures
The ERM team are continuously updating instructions and procedures. The decided dimensions for risk evaluation and their corresponding grading, the structured ERM reporting process, aggregation levels, impact areas evaluations, and total risk score are examples that instructions and procedures are used in the aggregation process.

Risk Information
Risk information should be presented to the system level in accordance with instructions and procedures from the system level, according to Hassel (2018). Risk information is discussed separately in section 6.1.5.

Aggregation Mechanism
As explained in section 5.9, aggregation is at times conducted within functions before risks are communicated to the ERM team. However, since the framework by Hassel (2018) is applied where functions are regarded as sub-system level and the ERM team as the system level, the aggregation mechanisms and additional analytical activities refer to the activities conducted by the ERM team (explained in chapter 5), e.g. evaluating aggregation levels of risks.

Support Needs and Providing Support
It was observed during the ERM reporting process that functions expressed what support they needed to report risks in accordance with guidelines from the ERM team. RC is essential for functions to express what support they need. Functions are encouraged to send questions and ask for help outside RC meetings. From observations in RC meetings, no indications were seen that support from ERM team was insufficient to meet the support needs that functions expressed.

In line with recommendations by Hassel (2018), sub-system levels are not solving problems related to risk information or risk aggregation by themselves. This was concluded from observations in RC meetings. Since the ERM team are continuously updating and improving the ERM work, it seems to be preferred by RC members that ERM team solve issues centrally.

Information/Knowledge Basis
Communication in general is prioritized in the ERM team. Available information that can be useful for functions is conveyed by the ERM team in RC meetings or by other means of communication. However, it was discovered that the ERM team do not always have necessary information. There are functions working with collecting information regarding ongoing events worldwide, e.g., relating to markets or geopolitics. As the ERM team do not have resources to

conduct such information collection, this information should be shared with the ERM team. The information could be distributed to functions by the ERM team. However, since aggregation is conducted within the same organization, information/knowledge basis is believed to be more accessible compared to the context Hassel (2018) describes where the main part of sub-systems are external actors.

6.1.5 Risk Information

The availability and quality of risk information is central in risk aggregation according to Jankensgård (2019), Månsson et al. (2015), Månsson et al. (2019) and Hassel (2018). From the additional literature, it was concluded that the following aspects are central regarding risk information.

Uncommon Risk Information
As described in section 4.2 and section 4.3, uncommon risk information creates difficulties in synthesizing risk information, and mixing risk descriptions is especially negative for large companies. It is unclear what large refers to, but the case company likely qualifies as large, thus it is important to avoid mixing risk descriptions.

It was observed during the consolidation workshop that risks reported to the ERM team varied in amount and detail level regarding the information provided with each risk. There were risks that did not contain information at all, apart from a sentence describing the risk. Other risks had necessary gradings and long descriptions of the risks. Of the seven types of risk information that should be provided with each risk (see section 5.8), uncommon categorization was mainly problematic in risk descriptions. Uncommon categorization in risk descriptions could partly be due to unspecific guidelines. Instructions on how risk information should be presented are clearer in the remaining six areas. However, risk information was increasing in amount further up in the ERM hierarchy as more information was added when risks were forwarded in the ERM reporting process.

Common Grading
Even if risk information is uncommon, it is helpful that the official guidelines from the ERM team states that all risks should contain the impact dimensions and corresponding grading. Using quantitative estimates is usually preferred over qualitative as Månsson et al. (2019) argue. It should be noted that implementing advanced quantitative elements may not be preferred, as Peter (2008) argues. Hence, using basic quantitative gradings like the case company seems to be the correct approach.

Background Knowledge
As Månsson et al. (2015) argue, lacking background information contributes to difficulties in synthesizing information. If reported risks contain grading of the impact dimensions (Table B.1 in Appendix B), it can still be difficult for the ERM team to understand what assumptions the gradings are based on if there is no background knowledge provided. In cases where reported risks are already aggregated, it is preferred if there is background knowledge of the risks in isolation and in combination with each other as Bjørnsen and Aven (2015) argue. In multiple cases, reported risks to the ERM team did not contain background knowledge of what

aggregated risks it is composed of. For example, if a reported risk was a level two risk, it was common that the description did not contain information of what level three risks it was composed of. It is difficult for the ERM team to properly aggregate level two risks with eachother if they do not know what level three risks they are composed of. The general impression from observing reported risks was that background information was less priortized than the impact dimensions and corresponding gradings.

Connection to Events or Scenarios

It was observed in the consolidation workshop, in ERM core meetings and in RC meetings, that several risks had weak connections to events or scenarios in their title and/or risk description. The risk descriptions could contain rather much information but lack this connection. What multiple definitions of risk have in common is that risk is equal to the events or scenarios, the consequences from the events or scenarios, and their associated probabilities (Aven, 2010). Månsson et al. (2015) argue that without scenarios in RVAs, it is difficult to compare actors in terms of vulnerability and the level of risk they are facing. Månsson et al. (2015) further argue that it is difficult to identify efficient reduction measures for risk and vulnerability if scenarios are not used as they function as reference points. If risks are not connected to events or scenarios, it will hence be difficult to not only identify vulnerability and risk reduction measures, but also to aggregate risks.

6.2 Improvement Suggestions

This section provides improvement suggestions based on the analysis in section 6.1.

6.2.1 Investigate Impact of Absence of a CRO

As explained in section 6.1.2, the current risk management officer leading the ERM team is not a C-level executive as a CRO described in literature. Since the literature highlights the CRO within ERM, it should be investigated what impact the absence of a CRO has on ERM in the case company. Understanding this impact could lead to future improvements.

6.2.2 Risk Selection

As argued in section 6.1.3 it is not realistic to eliminate risk selection (utilized to prioritize risks) in the ERM reporting process, instead it could be improved:

- Investigate what underlying risks the selected risks are composed of. Try to utilize aggregation in the selected risks to represent overall risk exposure
- Be aware, especially in risk selection situations, of what risks that tend to be under-managed and over-managed
- Create awareness of the hierarchy of risk management and identify potential conflicting objectives
- Estimate impact of risks in workshops where several people are involved as it is difficult for functions to estimate if there is impact on other functions. Workshops could reduce conflicts (e.g., objectives of functions and objectives of the organization) and to detect interdependencies between stakeholders.
- Investigate to use a method in combination with risk scores, e.g. prioritizing risks based on the VRIN criteria (explained in section 3.9.1).

6.2.3 Aggregation of Risk Information

Information/knowledge basis (in the framework by Hassel, 2018) can be improved for the ERM team. There is information available in the company regarding events related to markets and geopolitics. ERM would benefit from this information, e.g., outlook of risks could be better estimated with access to such information.

6.2.4 Risk Information

Uncommon categorization was mainly problematic in risk descriptions where the background knowledge that was provided was insufficient at times to understand the risks. The recommendation to improve the risk descriptions is to create clearer guidelines on what risk descriptions should contain, which can reduce uncommon categorization. Risk descriptions should include descriptions of the events or scenarios.

6.2.5 Connection to Events or Scenarios

As explained in section 6.1.5, basing risks on events or scenarios is essential according to Aven (2010) and Månsson et al. (2015). To make sure risks are based on events, basic methods can be used, e.g. the risk triplet by Kaplan and Garrick (1981). The risk triplet encompasses what Aven (2010) argues that most risk definitions include, i.e. the events or scenarios, the consequences from the events or scenarios, and their associated probabilities. The risk triplet is three questions that should be answered:

1. What can happen?
2. How likely is it that it will happen?
3. If it does happen, what are the consequences?

Answering the first question helps to define the event. The third question facilitate the distinction between events and consequences, which are sometimes used interchangeably. Separating the two is important to decide on correct mitigation activities as they should be utilized before the consequences occurs. Creating stronger connections to events facilitates the understanding of risks, identification of vulnerability- and risk reduction measures, impacts on other functions, and aggregation of risks.

Clarity in Event Descriptions

Another method to further improve the act of defining events or scenarios is to use the "clarity test" by Howard (1988): Would a clairvoyant who knew the future be able to determine if an event occurred or not? For example, in the event of "raw material prices increase" it would be difficult to answer. The event is better described as what raw material that is of interest, how large the price increase should be in reference to a value, and during what time period. The event could thus be expressed as "Steel price increase of X % compared to base price Y SEK/ton during the time period Z". In the future it would be possible to determine if the event occurred or not.

Clarity in events leaves less room for interpretation and enables improvements since it is possible to follow up on clearly defined events. If KRIs are to be implemented, there must be something to measure. If risks are described too general, they are difficult to monitor by measurements and it is difficult to address correct mitigation strategies. Furthermore, clear events are traceable after aggregation. Later in time, it may be necessary to trace what sub-events an event is composed of, e.g. if an event is realized, what sub-event triggered it?

7 Conclusions

Three research questions were formulated for the thesis. Conclusions regarding the literature in the scoping study is made by answering RQ1:

- Articles in Group A investigate the relationship between ERM and financial indicators. Most articles show a positive relationship between the two, but the cause-effect relationships are not clearly established.
- Articles in Group B and C provided valuable information on why certain aspects of ERM are important, but less on how ERM should be conducted in practice.
- Additional literature on risk aggregation in other contexts was available and considered to be applicable in ERM contexts. Considering that only one article explicitly addressed risk aggregation in the scoping study, i.e. in ERM contexts, while there is literature available on risk aggregation in other contexts, it indicates there is a gap in ERM literature regarding risk aggregation.

RQ2 was answered by investigating ERM in practice, with emphasis on risk aggregation, at a case company:

- There are procedures and organizational roles for ERM in the case company, e.g. the risk committee, centralized ERM team, risk owners etc.
- Risk evaluation is conducted against risk dimensions (e.g. impact area and vulnerability) but also against business plan and strategy.
- Risk aggregation is used in combination with selecting what risks to forward in the ERM reporting process, to reduce the number of risks into manageable amounts.
- Several procedures and guidelines are in place for risk aggregation, e.g. aggregation levels.
- Essential components for risk aggregation in literature aligns with findings in the company.

RQ3 was answered by comparing findings in the case company with the literature:

- Findings in the case company aligns with the literature in several areas, e.g. ERM integration with strategy and objectives, hence not all areas should be targeted for improvements.
- Investigate what impact the absence of a CRO has on the company.
- The process of selecting what risks to prioritize can be improved by being aware of biases, utilize workshops, investigate to use additional methods, e.g. the VRIN criteria.
- Risk description in risk information can be improved as providing background knowledge and commonality in information is beneficial for risk aggregation.
- The connection between risks and events can be stronger as it is weak at times. Strong connection to events provides several benefits.

Numerous central aspects of ERM in the reviewed literature aligned with findings on ERM in the case company. The findings also show that risk aggregation is necessary to not overload higher management and board of directors with information since many risks are identified.

The findings in this thesis are not representative for companies in general since only one company is investigated. However, the findings on risk aggregation in the case company in combination with the limited findings of risk aggregation in the ERM literature, indicate there is a need for further research on risk aggregation in ERM contexts. It is unknown why there is more literature on risk aggregation in other contexts than in ERM contexts. There is no reason to believe that risk aggregation is of less importance in ERM.

Since the ERM concept is encompassing it is likely more suitable to narrow the scope when ERM is investigated, perhaps to select one specific topic within ERM and risk aggregation. However, examining isolated parts of ERM could lead to that the comprehensiveness of ERM is overlooked.

References

Al-Amri, K., & Davydov, Y. (2016). Testing the effectiveness of ERM: Evidence from operational losses. *Journal of Economics and Business, 87*, pp. 70-82.

Alviniussen, A., & Jankensgård, H. (2009). Enterprise Risk Budgeting: Bringing Risk Management Into the Financial Planning Process. *Journal of Applied Finance*(1&2), pp. 178-192.

Arena, M., Azzone, G., Cagno, E., Silvestri, A., & Trucco, P. (2014). A model for operationalizing ERM in project-based operations through dynamic capabilities. *International Journal of Energy Sector Management, 8*(2), pp. 178-197.

Arksey, H., & O'Malley, L. (2005). Scoping Studies: Towards a Methodological Framework. *International Journal of Social Research Methodology, 8*(1), pp. 19-32.

Aven, E., & Aven, T. (2015). On the Need for Rethinking Current Practice that Highlights Goal Achievement Risk in an Enterprise Context. *Risk Analysis, 35*(9), pp. 1706-1716.

Aven, T. (2010). On how to define, understand and describe risk. *Reliability Engineering and System Safety, 95*, pp. 623-631.

Baxter, R., Bedard, J. C., Hoitash, R., & Yezegel, A. (2013). Enterprise Risk Management Program Quality: Determinants, Value Relevance, and the Financial Crisis. *Contemporary Accounting Research, 30*(4), pp. 1264-1295.

Beerens, R. J., & Tehler, H. (2016). Scoping the field of disaster exercise evaluation - A literature overview and analysis. *International Journal of Disaster Risk Reduction*, pp. 413-446.

Bjørnsen, K., & Aven, T. (2019). Risk aggregation: What does it really mean? *Reliability Engineering and System Safety, 191*, pp. 106524.

Bogodistov, Y., & Wohlgemuth, V. (2017). Enterprise risk management: a capability-based perspective. *The Journal of Risk Finance, 18*(3), pp. 234-251.

Brown, I., Steen, A., & Foreman, J. (2009). Risk Management in Corporate Governance: A Review and Proposal. *Corporate Governance: An International Review, 17*(5), pp. 546-558.

Burnaby, P., & Hass, S. (2009). Ten steps to enterprise-wide risk management. *Corporate Governance: The international journal of business in society, 9*(5), pp. 539-550.

Callahan, C., & Soileau, J. (2017). Does Enterprise risk management enhance operating performance? *Advances in Accounting, 37*, pp. 122-139.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2004). *Enterprise Risk Management - Integrated Framework.* New York: COSO.

Dickinson, G. (2001). Enterprise Risk Management: Its Origins and Conceptual Foundation. *The Geneva Papers on Risk and Insurance. Issues and Practice., 26*(3), pp. 360-366.

Drew, S. A., Kelley, P. C., & Kendrick, T. (2006). CLASS: Five elements of corporate governance to manage strategic risk. *Business Horizons, 49*, pp. 127-138.

Farrell, M., & Gallagher, R. (2015). The Valuation Implications of Enterprise Risk Management Maturity. *Journal of Risk and Insurance, 82*(3), pp. 625-657.

Farrell, M., & Gallagher, R. (2019). Moderating influences on the ERM maturity-performance relationship. *Research in International Business and Finance, 47*, pp. 616-628.

Fraser, J. R., & Simkins, B. J. (2016). The challenges of and solutions for implementing enterprise risk management. *Business Horizons, 59*(6), pp. 689-698.

Frigo, M. L., & Anderson, R. J. (2011). Strategic risk management: A foundation for improving enterprise risk management and governance. *Journal of Corporate Accounting and Finance, 22*(3), pp. 81-88.

Gatzert, N., & Martin, M. (2015). DETERMINANTS AND VALUE OF ENTERPRISE RISK MANAGEMENT: EMPIRICAL EVIDENCE FROM THE LITERATURE. *Risk Management and Insurance Review, 18*(1), pp. 29-53.

Gordon, L. A., Loeb, M. P., & Tseng, C.-Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy, 28*(4), pp. 301-327.

Grace, M. F., Leverty, T., Philipps, R. D., & Shimpi, P. (2015). The Value of Investing in Enterprise Risk Management. *The Journal of Risk and Insurance, 82*(2), pp. 289-316.

Hassel, H. (2018). A framework for aggregating risk information across organizational levels - the case of Swedish municipalities. i S. Haugen, A. Barros, C. van Gulijk, T. Kongsvik, & J. E. Vinnem, *Safety and Reliability - Safe Societies in a Changing World - Proceedings of the 28th International European Safety and Reliability Conference, ESREL* (ss. pp. 1665-1672). London: CRC Press.

Howard, R. A. (1988). Decision Analysis: Practice and Promise. *Management Science, 34*(6), pp. 679-695.

Hoyt, R. E., & Liebenberg, A. P. (2011). The Value of Enterprise Risk Management. *Journal of Risk and Insurance, 78*(4), pp. 795-822.

Jalali, S., & Wohlin, C. (2012). Systematic literature studies: Database Searches vs. Backward Snowballing. *International Symposium on Empirical Software Engineering and Measurement*, pp. 29-38.

Jankensgård, H. (2019). A theory of enterprise risk management. *Corporate Governance (Bingley), 19*(3), pp. 565-579.

Kallenberg, K. (2009). Operational Risk Management in Swedish Industry: Emergence of a New Risk Paradigm? *Risk Management, 11*(2), 90-110.

Kaplan, S., & Garrick, B. J. (1981). On The Quantitative Definition of Risk. *Risk Analysis, 1*(1), pp. 11-27.

Kimbrough, R. L., & Componation, P. J. (2009). The Relationship Between Organizational Culture and Enterprise Risk Management. *Engineering Management Journal, 21*(2), pp. 18-26.

Lechner, P., & Gatzert, N. (2018). Determinants and value of enterprise risk management: empirical evidence from Germany. *The European Journal of Finance, 24*(10), pp. 867-887.

Lee, L. S., & Green, E. (2015). Systems Thinking and its Implications in Enterprise Risk Management. *Journal of information systems, 29*(2), pp. 195-210.

Lundqvist, S. A. (2014). An Exploratory Study of Enterprise Risk Management: Pillars of ERM. *Journal of Accounting, Auditing and Finance, 29*(3), pp. 393-429.

Lynch, G. S. (2008). *At Your Own Risk: How the Risk-conscious Culture Meets the Challenge of Business.* Hoboken, NJ: JohnWiley & Sons.

Malik, M. F., Zaman, M., & Buckby, S. (2020). Enterprise risk management and firm performance: Role of the risk committee. *Journal of Contemporary Accounting and Economics, 16*(1), pp. 100178.

McShane, M. K., Nair, A., & Rustambekov, E. (2011). Does Enterprise Risk Management Increase Firm Value? *Journal of Auditing & Finance, 26*(4), pp. 641-658.

Mensah, G. K., & Gottwald, W. D. (2016). ENTERPRISE RISK MANAGEMENT: FACTORS ASSOCIATED WITH EFFECTIVE IMPLEMENTATION. *Risk Governance and Control: Financial Markets and Institutions, 6*(4), pp. 175-206.

Mishra, B. K., Rolland, E., Satpathy, A., & Moore, M. (2019). A framework for enterprise risk identification and management: the resource-based view. *Managerial Auditing Journal, 34*(2), pp. 162-188.

Månsson, P., Abrahamsson, M., & Tehler, H. (2019). Aggregated risk: an experimental study on combining different ways of presenting risk information. *JOURNAL OF RISK RESEARCH, 22*(4), pp. 497-512.

Månsson, P., Abrahamsson, M., Hassel, H., & Tehler, H. (2015). On common terms with shared risks – Studying the communication of risk between local, regional and national authorities in Sweden. *International Journal of Disaster Risk Reduction, 13*, pp. 441-453.

O'Donnell, E. (2005). Enterprise risk management: A systems-thinking framework for the event identification phase. *International Journal of Accounting Information Systems, 6*, pp. 177-195.

Oliva, F. L. (2016). A maturity model for enterprise risk management. *Int. J. Production Economics, 173*, pp. 66-79.

Paape, L., & Speklé, R. F. (2012). The Adoption and Design of Enterprise Risk Management Practices: An Empirical Study. *European Accounting Review, 21*(3), pp. 533-564.

Peters, E. (2008). Numeracy and the Perception and Communication of Risk. *Annals of the New York Academy of Sciences*, pp. 1-7.

Tekathen, M., & Dechow, N. (2013). Enterprise risk management and continuous re-alignment in the pursuit of accountability: A German case. *Management Accounting Research, 24*, pp. 100-121.

Yin, R. K. (2003). *Case Study Research Design and Methods* (Third ed.). Thousand Oaks: Sage publications Inc.

Zou, X., Isa, C. R., & Rahman, M. (2019). Valuation of enterprise risk management in the manufacturing industry. *Total Quality Management, 30*(12), pp. 1389-1410.

Appendices

Appendix A and Appendix B are included in this chapter. Read each appendix for more details.

Appendix A. Excluded Subject Areas In Article Search on Scopus

The following subject areas were excluded from the article search on Scopus:

- Medicine
- Biochemistry, Genetics and Molecular Biology
- Immunology and Microbiology
- Pharmacology, Toxicology and Pharmaceutics
- Agricultural and Biological Sciences
- Social Sciences
- Neuroscience
- Chemistry
- Earth and Planetary Sciences
- Veterinary
- Physics and Astronomy
- Materials Science
- Chemical Engineering
- Dentistry
- Arts and Humanities
- Psychology
- Health Professions
- Nursing

Appendix B. Types of Risk Information

This Appendix presents the seven types of risk information in detail that should be provided with each risk. The seven types of risk information are mentioned but not presented in detail in section 5.8. The findings in this appendix are from guidelines for risk information created by the ERM team. The information in Table B.2 is from documentation for an ERM core team meeting.

Risk Description
The risk description should contain explanations and background information of risk. Elaborations on the reason to the risk and its outlook. Identified opportunities if the risk is managed successfully should also be included.

Risk Outlook
What is the outlook of the risk? How is the risk developing, is it increasing/decreasing or stable?

Risk Owner
Specification of who the risk owner is.

Risk Drivers and Monitoring
What are the external threats and uncertainties that are associated with the risk? What are the internal vulnerabilities and uncertainties that drives the risk? How can the risk be monitored? Are there KRIs? Which function is monitoring the KRIs?

Risk Evaluation
Risks should be evaluated based on the dimensions and gradings in Table B.1. Impact area is not graded as one or several areas are specified instead. The impact areas are illustrated in Figure B.1.

Table B.1. Impact areas in the evaluation model.

Dimension	Definition	Grading
Impact area	Impact areas illustrated in Figure B.1	N/A
Impact	Magnitude of the consequence	1-8
Vulnerability	Weakness within own control. Weakness leads to vulnerability towards threats	1-4
Threat	Potential event outside own control that could cause an impact	1-4
Likelihood	*Vulnerability + Threat*	1-8
Velocity	How fast a materialized risk impacts the organization	1-4

To systematically assign grades to risks, there are definitions of the gradings in the dimensions available, e.g. for vulnerability and threat, the grading is from Low (1) to Extreme (4).

The model to estimate impact is composed of six impact areas, displayed in Figure B.1. The impact areas are developed from core values. Impact levels for the areas have descriptions to assess what the impact level should be, see example in top left corner in Figure B.1.

		Impact areas					
		Health & Safety	Society	Planet & environment	Brand & reputation	Business Continuity	Financial
Impact level	8	Fatalities among customers, employees or others under the duty of care					
	7						
	6						
	5						
	4						
	3						
	2						
	1						

Figure B.1. Impact areas in the evaluation model.

If risks affect multiple of the six areas, the highest impact level is selected. For example, if a risk is estimated to have impact on Health & Safety at level 5 and on business continuity on level 4, the impact will be set to five on Health & Safety.

The gradings are subsequently used as guidance to what type of focus the risk will have:

- EM focus - Impact 7-8, likelihood 5-8
- EM awareness – Impact 7-8, likelihood 1-4
- Functional focus – Impact 5-6, likelihood 5-8
- Functional awareness – Impact 5-6, likelihood 1-4
- Below ERM threshold – Impact < 5

If impact is four or lower, risks are below the ERM “threshold”. Impact is the determining dimension as risks could have impact of four and a likelihood of five but still be below the ERM threshold. A formula to calculate total scores of risks is used to enable comparisons between risks and between points in time as well. The scores are central in deciding what risks to include in the top 20 list.

The outlook grading helps to monitor risks and how they are expected to develop. The outlook estimation is not connected to the score. Table B.2 shows how risks are presented in a heat map. The table is part of a larger heat map from an ERM core team meeting.

Table B.2. Example of risk with corresponding dimensions and scores.

Risk name	Impact	Threat	Vulnerability	Velocity	Outlook	Q4 score	Q2 score
Deteriorating macro economics	6	3	3	4	Increasing	144	90

The scores are updated during the ERM reporting process. New events or successful mitigation activities change the scores. The functions update previously known risks in every ERM reporting process. The focus of the ERM team is on residual risks and the only inherent risks that reaches the ERM team are new risks that are not mitigated yet.

Risk Response

Should contain countermeasures in place and who the responsible person is. If additional mitigation is required to achieve acceptable levels, it should be stated here. Decisions to be made or already made decisions regarding mitigation activities should be stated. Urgency of mitigation activities is included.

Risk Acceptance

Description of the accepted risk level. Maximum costs for mitigation and deciding person/forum for these activities should be stated.