STOCKHOLM SCHOOL OF ECONOMICS
Department of Accounting
BE351 Degree Project in Accounting and Financial Management
Spring 2025

Behind the Façade: Unveiling the Reality of ERM

Nils Julin (25778) and Emil Nilsson (25631)

Abstract: This study explores the practical implementation and managerial influence on Enterprise Risk Management (ERM) in a Swedish manufacturing firm. Although ERM frameworks such as COSO (2017) and ISO 31000:2018 are widely promoted, their real-world application often diverges from formal prescriptions, raising questions about their impact. This issue is particularly salient given that most prior research is centered around the financial industry, underscoring the need for more context-sensitive research. Adopting a qualitative single-case study approach and applying agency theory as an analytical lens, this paper examines how risk management is shaped by managerial discretion, internal control systems, and organizational culture. The findings reveal that risk management practices can be driven by intuition, experience, and informal delegation rather than quantitative measures or formal risk appetite. Moreover, the study highlights how ERM may serve as a symbolic tool, creating a façade of control whilst actual practices rely on interpersonal trust and selective oversight. By extending ERM research into the manufacturing sector, this paper contributes to a better understanding of risk management, revealing the tension between formal structure and interpretative managerial practices in shaping risk management.

Keywords: Enterprise Risk Management, managerial influence, agency theory, internal control systems, risk management

Supervisor: Gianluca Delfino, Assistant Professor at the SSE's Department of Accounting

Acknowledgements: We would like to express our sincere gratitude to all interviewees willing to participate in this study, who provided valuable insights enabling this thesis. We also want to thank our supervisor, Gianluca Delfino, for his invaluable feedback and support.

Table of Contents

1. Introduction

1.1 Background

Risk has long carried a negative association that preferably should be avoided or transferred to parties outside of the organization. Doing so entirely does however imply the forfeiting of pursuing organizational objectives. The International Organization for Standardization (ISO) has thus reframed the definition of risk as "a necessary part of doing business" (ISO, 2018). The term risk itself can encompass a broad spectrum of events and circumstances. For individuals, it may involve illness, property loss, or physical harm. In this paper, however, risk will refer specifically to threats faced by businesses, whether these are macroeconomic, environmental, operational, or reputational in nature (McKinsey and Company, 2023).

According to ISO (2018), the fundamental reason for businesses to manage risk from a performance perspective is that it increases their likelihood of achieving their objectives and increasing the protection of their assets. Keeping this perspective in mind, it is not surprising that awareness and consensus around risk and risk management tend to intensify following major crises. Notable examples include the 1998 framework introduced by the Basel Committee on Banking Supervision (2013) in response to the collapse of German and U.S. banks in 1974, as well as the second revision of this framework, which was developed in the aftermath of the 2007–2009 financial crisis (Bank for International Settlements, 2013, 2017). This trend is also reflected in academic discourse, particularly in the work of Michael Power, who identified a broader societal shift toward what he termed "the risk management of everything" (Power, 2004, p. 59).

A more interconnected business landscape, combined with the growing plausibility of external risks, has led many organizations to adopt Enterprise Risk Management (ERM) (McKinsey and Company, 2023). Compared to traditional risk management, ERM emphasizes a holistic perspective in which non-quantifiable risks are considered, ultimately taking a positive view by which the organization might pursue strategic opportunities that may arise (Lundqvist, 2014; Mikes, 2009; COSO, 2017). This broader trend toward more sophisticated methods for risk management has also driven the development of institutional frameworks for ERM

implementation, most notably the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) (2017) and ISO 31000:2018. Since its initial release, COSO has issued additional guidance on the use of the framework across various sectors and organizational contexts.

1.2 Problem formulation

Although frameworks like COSO (2017) and ISO 31000:2018 provide valuable guidance for organizational implementation of ERM, the translation from idea to practice of ERM systems within firms remains a significant challenge. Referencing COSO's 2001 "Report on ERM", Lundqvist (2014) highlights how flaws and inconsistencies within the guiding frameworks in reality creates disagreement on what ERM really is. She also highlights how there might be instances where firms unknowingly implement ERM dimensions, resulting in an underreporting of ERM practices, implementation and evaluation. This disagreement is also present in academia, whereby different definitions and measurement methods give rise to ambiguity in the definition of ERM (Lundqvist, 2014; Braumann et al., 2024; Mikes, 2009). Naturally this has resulted in criticism against the framework, accusing it of being hollow and symbolic, potentially obscuring rather than highlighting risks (Power, 2009).

The field lacks a nuanced, industry-specific understanding of ERM as a majority of literature is either focused on ERM as a conceptual framework or its applications within the financial industry. Despite being limited to the context of Tehran's Stock Exchange, Fasihi et. al. (2022) highlights the need for research adopting a broader view with a focus on context-specific challenges. This is further emphasized by increasingly interconnected global business environments, where external threats pose different risks to supply chains than those typically encountered in service-based industries (OECD, 2013, p. 197). Together with calls for qualitative and context-sensitive studies, this paper seeks to address these challenges by examining how ERM is implemented in a manufacturing firm, the adequacy of existing ERM frameworks, and how risk is managed in practice (Lundqvist, 2014; Arena et al., 2010; Mikes, 2009; Fasihi et. al, 2022).

1.3 Aim and research question

The aim of this paper is to investigate what aspects of Enterprise Risk Management (ERM) are implemented within manufacturing firms. We intend to explore how the indicative risks are

interpreted and acted upon in day-to-day operations, as well as what measures are taken to mitigate them. Furthermore, we will analyze how managerial influence plays into the construction of risk measures and delegation of risk ownership within the hierarchical organization. Drawing on qualitative insights from a manufacturing firm, this study explores how ERM is implemented and experienced in practice, leading to the following research questions:

I. How is Enterprise Risk Management (ERM) implemented in manufacturing firms, and what specific aspects of risk are prioritized and acted upon in day-to-day operations?

The question above will lay the foundation for a further discussion as to why the implementations have taken place, what actors that involved, as well where within the hierarchical context of the organization responsibility for these measures ultimately lies. This discussion will enable the answering of the second research question:

II. To what extent does managerial influence shape the construction of risk measures and the delegation of risk ownership within the hierarchical structure of manufacturing firms, and how does this impact the organization's overall risk management practices?

To interpret our findings, we adopt agency theory as an analytical lens. Given the scope of the research being to analyze the potentially discretionary nature of risk management practices, agency theory provides a useful framework for analyzing authority, incentives, and how accountability is distributed. It enables a structured exploration of how managerial influence interacts with formal frameworks, especially in contexts where ERM may function both as a control system and a symbolic practice.

1.4 Contribution

This study contributes to the ERM literature by extending the focus beyond financial services into other industries, thereby responding to calls for a more context-sensitive approach to risk management. By examining the role of managerial influence in the construction of risk measures and delegation of risk ownership within the organizational hierarchy, this paper also adds depth to the stream of research that views ERM as a symbolic and interpretive practice.

As a consequence, this paper challenges the view of ERM as a rigid and prescriptive framework.

2. Theoretical development

2.1 Understanding Enterprise Risk Management

Enterprise risk management (ERM) emerged as a shift in organizational thinking, primarily driven by a growing public interest in corporate governance and demands for greater transparency on risk-based internal control systems. As Power (2004, p. 59) describes, it was a broader “project of turning organizations "inside out"”, reflecting how internal controls became a more visible and moral obligation. This shift coincided with a trend toward government regulation that focused on rigid internal control systems, laying the foundation for prominent frameworks such as the Bank for International Settlements (2017) Basel banking accords, the COSO (2017) framework, and ISO 31000:2018.

Despite this regulatory momentum, there are notable discrepancies in the frameworks, particularly in terms of the components of ERM and how it best is implemented. As Lundqvist (2014) observed, this has resulted in firms developing internal processes, often guided by one or more of the external frameworks. Consequently, there is little consensus on what constitutes best practice, both between individual organizations and among experts. Nevertheless, Soin and Collier (2013) observed an over-arching theme in literature that risk management has moved away from the traditional and fragmented view of risk as silos, to being a central concern in need of management control. One way to understand this shift is by examining how organizations conceptualize and organize risk, moving from fragmented siloed approaches to more integrated and strategically informed control mechanisms.

2.1.1 From silos to integrated control

Risk-silos refer to the management of risks in isolation from one another, typically along functional lines, where each risk type is quantified, measured, and controlled independently. Whilst this approach is most prominent in the financial industry, especially in the measurement of market risk, it has been applied in other sectors as well. In accounting, a silo perspective

might entail the focus on financial statement disclosures, without the incorporation of broader strategic or operational risks (Mikes, 2009; Soin and Collier, 2013).

Mikes (2009; 2011) described how risk-silo management is one of four ideal types of risk management. The first two types of ideal risk management concern the way of counting, whereby silos constitute the categorization and quantification of risks. One example of risk-silo management is the surveillance of currencies in the category of market risk (Drzik et al., 2004), with a frequently used method being value-at-risk (VaR) (Jorion, 1997). The second type of ideal risk management concerning the way of counting is integrated risk management, or risk aggregation. This implies that a common denominator is attached to the various silos such that firms can aggregate all quantifiable risk into a total risk estimate. The development of economic capital (also known as economic risk capital), a measure describing the estimated capital requirement to cover all liabilities in case of a severe loss event, enabled practitioners to aggregate risk from product level all the way through to the organization at large (Mikes 2009; 2011).

The two remaining types of ideal risk management as presented by Mikes (2009; 2011) concern the way risks are managed. Mikes (2011) propose that risk can either be managed by a strong shareholder value imperative or by a risk-based internal control imperative. Managing risks through the lens of shareholder value is what Mikes refers to as risk-based management, in which business units are evaluated based on the additional return they generate for shareholders relative to the quantifiable risk they incur. Lastly, managing risks based through an internal control imperative includes the notion that non-quantifiable risks must be managed as well. This is exemplified by highlighting risks that materialize rarely, such as the risk of strategic failure or reputational risks. The nature of these risks make the mitigation techniques somewhat arbitrary as they require an act of judgement, experience, and intuition (Mikes, 2009). Whilst Mikes' typology helps clarify the conceptual boundaries of ERM, it does not by itself capture how ERM is operationalized within organizations. In practice, the adoption of ERM frameworks often reflects both structural components and varying degrees of managerial interpretation.

2.1.2 The dimensions of ERM: From framework to practice

Lundqvist (2014) observed in her survey that the many interpretations of ERM stem from the framework itself lacking clarity in terms of definition and way of implementation, with more than a third of respondents highlighting that they, either solely or in combination with other frameworks, develop internal frameworks in order to implement ERM. This highlights how ERM is adopted might differ between organizations, creating a subsequent uncertainty on what ERM really is and how it should be implemented (Lundqvist, 2014). As a result, Lundqvist (2014) identified four pillars required for ERM to be considered implemented.

The two first components are not directly connected to risk management or ERM, but more so to the general declaration of objectives and monitoring of internal activities. Examples include the documentation of policies and procedures, channels of communication, and stipulated performance goals to achieve its objectives. Thus, organizations may have fully implemented these pillars without explicitly trying to implement holistic ERM. The fourth component is concerned with the considerations of a variety of risks, but still fails to differentiate whether the organization at hand has implemented ERM or uses risk-silos. It is therefore the third component that differentiates firms that succeed at fully implementing ERM from those who do not (Lundqvist, 2014).

In order for a firm to have fully implemented ERM, not only must it have the appropriate organizational structure and identification of risks in place, it must also approach risk management the way ERM prescribes (Lundqvist, 2014; COSO, 2017; ISO 31000:2018). The third and final pillar thus includes having a formal written statement of risk appetite, a centralized department or staff function dedicated to risk management, and alternative risk responses for each significant event. Only when all four pillars are present and properly functioning the firm can be considered to have implemented ERM, despite not all of the pillars being specific to ERM or risk management in isolation (Lundqvist, 2014).

2.1.3 ERM as an interpretative and organizational practice

Calculative cultures are described by Mikes (2009) as the way organizations approach ERM depending on their inherent attitudes towards quantifiability. Mikes describes two separate cultures; namely quantitative enthusiasts, and quantitative sceptics, the first of which rely heavily on quantifiable risk metrics and risk models in their ERM approach, whilst the second

relies more on judgement, discussion, and informal controls. It is also explained that these separate cultures often see risk a bit differently. Apart from calculative cultures ultimately shaping managerial preferences toward ERM, something that will be discussed in the next section, calculative cultures also affect the way ERM is interpreted and implemented across firms (Mikes, 2009). As a result, in contrast to what regulatory frameworks suggest, the implementation of ERM may be more along the lines of an interpretative practice which is shaped by contextual adaptation and symbolism (Mikes, 2009; Hall et al., 2015). Power (2009) describes how the accounting-driven nature of the COSO-framework opens the door for detailed control, thereby running the risk of turning ERM into a box-checking practice for the mere practice of documenting the adherence to these controls. Similarly, this might lead to a form of measurement ritualism whereby risk metrics are constructed and legitimized primarily for their own sake, rather than serving a clear managerial purpose (Mikes, 2011). Despite being derived from the world of politics, these discrepancies might create opportunities for blame avoidance through delegation (Hood, 2002).

There are however indications that delegation of risk results in value creation. As noted by Mikes (2009, p. 25) the "performance of business units is measured relative to the quantifiable risk they incur. Pushing these performance measurements down to business units, products and even transactions gave rise to further potentially value-enhancing practices, such as risk pricing, risk transfer and portfolio risk management". One could theorize a delegation of this character could nurture interaction and dialog that ultimately results in the management of holistic risk, raising the question of the importance of practical tools such as risk maps in creating a meeting place for mediating interests and concerns (Mikes, 2011; Jordan et al., 2013).

Regardless of whether ERM develops into a meaningful control system or remains a symbolic exercise, the preceding research highlights how ERM is far from a fixed model, suggesting that it rather evolves through the interpretations and applications among managers. Managerial influence thus seems to play a key part of risk governance within their respective organizations (Mikes, 2009).

2.2 The role of managers in Enterprise Risk Management

In the article by Mikes (2009, p. 22), it is mentioned that "senior risk officers develop personal philosophies about the manageability of risks, and shape the composition of the risk management mix accordingly. Thus, a particular calculative culture both influences and is influenced by senior managers' choice and use of analytical models.". This insinuates that risk management is not objective but rather changes significantly based on the person behind the decisions. This sentiment of subjectivity in the decision making is further strengthened by Grant and Nilsson (2020) claim that strategic and financial rationales are fundamental to investment decisions. They note that "having experience when making forecasts and judgments based on expertise as having Fingerspitzengefühl." (Grant and Nilsson, 2020, p. 13). The judgments which lie as a base for strategic and financial rationales are, according to Grant and Nilsson (2020, p. 2), "based on a myriad of factors and data concretized into rough estimates", insinuating that extensive decisions are made by managers quite subjectively, mainly by intuition coming from expertise.

This influence is elaborated on further by Ittner and Oyon (2020) in their article about risk ownership. They put emphasis on the choices surrounding risk ownership as having a strong connection to the sophistication of ERM practices within a firm. Importantly, the authors point to the fact that the risk-owners of a firm possess the authority to make key decisions, and the authors also come to the conclusion that having more senior risk owners is beneficial to the functionality and sophistication of the ERM by limiting the biases which could be in place if only a single risk-owner took the correlated decisions. At first glance, this might appear to be in direct opposition to the findings of Mikes (2009), and Grant and Nilsson (2020), but in actuality, it provides us with a more refined approach to when ERM practices work the best and tells us that managers' intuition is a great resource, but with the caveat of there needing to be multiple in order to mitigate the risk of managerial biases in and of themselves.

Hall et al. (2015) contributes to the perspective by studying how risk managers influence decision makers within their organizations. They introduce the concept of toolmaking, which refers to how managers change and improve the practices surrounding the recording, collection, interpretation, and quantification of risk. The article provides insights into how risk managers use toolmaking, as well as interpersonal connections, to put their own influence on decision makers, this provides us with a new concept of how influence is maintained. Hall et al. provides

examples of two risk managers in banks, which give further interesting understandings, as in one bank, tools were found as communicable, adaptable, and well-integrated, whilst the other bank heavily relied on overly technical models, or simply through personal expertise, more or less neglecting tools. These examples show us two definitely separate types of approaches to risk management, which adds to the findings of Mikes (2009;2011) in regard to the existence of separate calculative cultures. The first way of using the tools is easier to implement at a group level, whilst the second way is, according to the article, a way of keeping relevance for the risk manager, as they are needed to, for example, decipher and interpret the outputs of models.

2.3 Theoretical framework

This study draws on agency theory to better understand how risk management structures interact with managerial influence in the context of ERM. Agency theory is particularly relevant when exploring settings where their authority is delegated and decision-making is decentralized, with the resulting outcome thus becoming harder to control. The theory is also well suited for organizational settings with goal incongruence between professionals, risk, and where performance evaluation is difficult (Eisenhardt, 1989). Because ERM involves both formal frameworks and managerial discretion, agency theory offers a useful lens for examining how risk governance unfolds in practice (Mikes, 2009; Hall et al. 2015). The following section outlines the core assumptions of agency theory, what risks are associated with delegation of authority and how these relate to ERM. The section concludes by highlighting the associated costs with agent monitoring and how agency theory previously has been applied in literature.

In its classical form, agency theory describes the relationship in which principals (e.g. a board of directors) delegate some decision-making authority to agents (e.g. managers) in order for them to perform tasks on their behalf (Jensen and Meckling, 1976). This implies that the agent is to provide his skills at the disposal for the principal's goal, disregarding any other objectives outside of this relationship. A key problem arises in ensuring that the preceding notion actually holds, as under the assumption of both parties maximizing their utility, there is no reason to believe that the agent will always act in the interest of the principal – also referred to as the agency problem (Mitnick, 1975; Jensen and Meckling, 1976; Eisenhardt, 1989).

The agency problem might semblance either in the form of moral hazard or adverse selection, by which the principal according to Eisenhardt (1989) has two options on how to proceed. The first is to utilize information systems such budgeting systems, reporting procedures, and additional layers of management to detect any deviant behavior of the agent. These information systems closely tie into Lundqvist's (2014) two first pillars of ERM which regard general internal environment and control activities. The second option is to align incentives by providing the agent with an outcome-based contract at the price of him bearing some of the organizational risk. This may create challenges when principals and agents differ in risk preferences, or when participative approaches to strategic and operational planning are culturally valued as a complement to incentive contracting, such as in Germanic and Nordic settings (Eisenhardt, 1989; Malmi et al., 2020).

Despite the efforts to align interests through information systems or outcome-based contracts, agents may still act opportunistically due to the non-zero cost and ineffective nature of these contracts (Perrow, 1986; Jensen and Meckling, 1976). One example of how systems aimed at aligning incentives can open the door for opportunistic behaviors can be found in bonus contracts, where agents may manipulate accruals to maximize their own rewards (Healy, 1985). Building on this, the notion of moral hazard, by which an agent conceals shirking behind the complexity or difficulty of being monitored, helps explain how symbolic applications of ERM can emerge to provide the appearance of compliance (Eisenhardt, 1989; Power, 2009; Mikes, 2011).

These limitations are not merely challenges of implementation, but point to a deeper theoretical assumption. Perfect alignment between the principal and the agent is fundamentally unattainable without incurring costs. This is also referred to as agency costs, and include the monitoring expenditures by the principal, the bonding costs for the agent, as well as a residual loss that describes the cost of the agent diverging from the principal's objectives (Jensen and Meckling, 1976). Due to the costly nature of monitoring, this means it might in principle not even be economically viable to monitor the actions of a large number of agents (Perrow, 1986; Ross, 1973).

Agency theory has been widely applied in studies of corporate governance, risk management, and internal control, providing credibility as a theoretical framework for this paper. For example, Adams (1994) used agency theory to explain the role of internal audit functions,

Shleifer and Vishny (1997) explored how corporate governance addresses the agency problem, and Bonner and Sprinkle (2002) analyzed how monetary incentives affect effort. More recent studies apply the theory in more subtle ways, such as how Ittner and Oyon's (2020) introduction of risk ownership can be perceived as a form of incentive alignment, and Hall et al.'s (2015) portrayal of managers as "toolmakers" who's shape decision-making through their interpretations of risk mitigating systems. Given the dual nature of ERM, which is influenced both by formalized frameworks and managerial practice, agency theory offers a robust foundation for interpreting its implementation within organizations.

3. Research methodology

In this chapter, the applied methodology used in this study will be presented. Section 3.1 details the research design and provides a rationale and justification for the appropriateness of the selected method. In Section 3.2, the used data-collection methods are described, the tools and techniques employed to gather relevant information are presented, along with the rationale behind. Lastly, Section 3.3 provides an overview of the data analysis.

3.1 Research design

In order to systematically address the research questions, a qualitative research design was adopted. This approach is described as being especially suitable for studies that seek to understand the role of accounting in its organizational and social context (Lee and Humphrey, 2006). Because we want to understand these contexts on a practical level within these organizational and social contexts, a qualitative research design was deemed the most appropriate.

Furthermore, a single qualitative case study approach was selected. According to Yin (2009) the case study methodology is suitable and appropriate when researching complex processes and phenomenon's within their real-world context, as it allows for very detailed exploration within the subject, a sentiment which is shared by Lee and Humphrey (2006), and Cooper and Morgan (2008). As a consequence, it was believed that this approach was the most appropriate for our study, as the study itself focuses on understanding complex phenomena in a real-world business setting on an organizational level. We felt this approach gave a possibility to reach even further exploratory depths, rather than a comparative breadth, felt to be associated with

the multiple case study approach. Another factor for choosing a single case study approach is the limited research timeframe.

In this study, an abductive approach will be adopted to facilitate the complex interplay between managers, risk owners, and the overall risk management approach of the corporation. Another aspect is the influence of managerial intuition in the decisions, and how this intuition complements or contrasts these traditional models. This will, in turn, allow the development of new insights based on the empirical data gathered from semi-structured interviews with the chosen company. The analysis will mainly be based on an organizational level, as our research question aims to understand how risk is managed, understood, and acted upon within the corporation rather than in a broader industry context. Whilst individuals, teams, and their understandings are used in the analysis, the insights drawn are instead used to understand the organizational approach to risk management and how this is shaped by individuals, culture, and leadership.

The study will be conducted within a medium to large-sized company, as such firms typically possess the complexity in processes required for a thorough analysis of the risk management. It was chosen to focus on corporations that conduct manufacturing due to us finding their risk profile very interesting and distinct, as there is plenty of research on risk management in the service industries for example. Whilst the company's production location is not a factor of utmost importance, the aim was to select an organization where risk management decisions are made in Sweden or culturally similar European countries. This choice was made based on our cultural familiarity with these regions, which helps to minimize potential misunderstandings due to linguistic or cultural differences.

To gather sufficient data, two rounds of semi-structured interviews were conducted with management. The first round was to gain insight on the firm as a whole and their practices and to find tensions within. Whilst the second round sought to gain further insight about the tensions that were found, and to uncover the perspectives, and practices surrounding risk management that arose from these tensions. This method was chosen because it provides the flexibility to explore topics in depth, whilst allowing for follow-up questions that can probe into the role of for example, intuition in decision-making. The interviews were conducted via video platforms (e.g., Teams), ensuring adaptability whilst maintaining the nuance of personal interaction.

Agency theory serves as our method theory and has provided us with a structural lens with which we can analyze and examine how the delegation, incentives, culture, and monitoring operate within the firm. The lens enables us to observe how well risk-related behavior, and the decision-making that surrounds it, aligns with theoretical expectations of the agent-principal relationship.

3.2 Data collection

As previously mentioned, we felt that we wanted to conduct research within a Swedish, medium to large-sized manufacturing firm as the main part of ERM research fell within service industries. We felt that the case study firm, Delta[1], which will be introduced further in later sections, was a good fit for our criteria. Given our studies focus on managerial discretion and intuition in risk-based activities, we felt it to be of utmost importance to interview those in managerial and executive positions, who are expected to make risk-based decisions. We therefore chose to interview Delta's Head of Business Control, who henceforth will be referred to as "The Manager". When describing his own role, the Manager explains that he is "*the right hand of the CFO*". We also performed an interview with Delta's Chief Financial Officer, henceforth referred to as "The CFO". These interviewees were identified to be relevant for our scope as they are involved in offer preparations, monitoring, and strategic oversight (see Appendix 1 for interviews). The interviews were conducted as semi-structured, as this allowed for flexibility in the form of follow-up questions where it was deemed necessary. Interview questions were based on previous interviews, domain, and method theory (see Appendix 2 for an interview guide example).

3.3 Data analysis

During each interview, respondents were asked if they approved being recorded, and as a result, 6 of the 7 interviews were, and shortly after, they were transcribed so that no contextual details or nuances were lost. The interview with the CFO was not recorded upon their request, and instead one of us asked questions, whilst both wrote down the CFO's answers, and coordinated the notes afterwards. All interviews were held in Swedish, and excerpts in form of quotes have been translated as carefully as possible in order to maintain the core and nuances of the quote.

[1] Pseudonymized name.

After each interview and transcription, we gathered to have a post-interview discussion to reflect upon impressions, emerging themes, and to clarify interpretations. If any simpler clarification was needed, emails were sent to the respondents at Delta. As our analysis progressed further, our approach became more and more iterative and reflexive as described in Srivastava and Hopwood (2009). Rather than seeing interviews as standalones, we constantly went back to material from earlier interviews to analyze new material and emerging patterns. What was found to be of interest during these post-interview analysis-based discussions, the clarifying emails to Delta, and together with relevant theoretical material, formed the basis of future interview questions. In some cases, revisions to the theory were taken if we felt that interesting topics were covered during interviews, but that we lacked sufficient theoretical backing for. This to ensure that for the subsequent interviews, we could explore further and deeper into what was deemed relevant.

4. Empirical analysis

4.1 Practices and risk landscape

4.1.1 Introduction to case company

The case company Delta is a multinational original equipment manufacturing firm, which has production and service facilities in 13 countries. The firm has four distinct business units holding significant market shares in and of their own. The largest of these business units holds an approximate 33% of its global segment. Some, if not most of the product offerings are very technically intricate requiring long-term detailed and difficult R&D. The project sizes usually range from 10-100 MSEK, and the firm has 500-1000 projects running parallel at all times. The company prides itself in "*...geographically being in the same place as our customers…*" (Manager), which in turn gives them a short time to market, providing them with a competitive advantage towards industry neighbours. These factors have resulted in a rapid growth which has brought with it a wide array of operational, financial, and strategic risks.

4.1.2 Complex products, complex risks

The Manager is under the impression that "*the operational apparatus is a bit too complex and we have a bit too high of a degree of refinement*", which in turn could be considered a main

operational risk. Moreover, the Manager explains that there is a large inherent risk in operating the way they do, with a high amount of tailormade R&D-solutions, as they are difficult to sell to other consumers, and there is potential for "*an unhealthy capital tie-up*" in inventory. The combination of a complex operational apparatus, low reusability among projects, and the large-scale production could potentially result in operational inefficiencies, unpredictabilities, and financial strains.

Technical risk, mainly in the form of the internal R&D and tailor-made technical solutions is mentioned by the CFO as one of the major hurdles to manage in Delta, and he explains that;

> " *...technical risks are very difficult to handle, you have to work through what the customers really want and really understand it so that it doesn't turn out wrong … it is very easy to make a fool out of yourself when you have already spent a lot of hours in the design*" (CFO).

One mitigating factor according to the CFO is to, already in the firm's internal pricing and bidding tool, henceforth referred to as the "P-Calc", add extra design-hours for customers who they know require more difficult designs, or who they suspect require a lot of changes. This complexity also follows into regulatory and compliance dimensions. The Manager explains that "*It's difficult to be centrally governed with all of the local exceptions and regulations that one has to take into consideration.*" He explains that Delta has to have strong internal audits and internal controls to mitigate the risks that come with a central governing body.

4.1.3 Financial risks

The Manager explains that another overlying risk is the liquidity, they explain that "*We have very large financial loans, and as a result also large quarterly interest-payments which can become challenging, especially when we don't get paid in time from our customers in the way that is stipulated in our contracts.*". On the same note, the Manager explains the following about the change in general industry conditions in regard to payments;

> "*Pre-payments have decreased within the industry during the last 15 years. Before 30% was not unusual, whilst now the mean is closer to 10%. One big reason is that the governmental customers have become more restrictive in their spending … There is a*

general industry demand to be cash-neutral, but we (Delta) *only secure this cash-neutral position when customers are on the brink of bankruptcy, and then we demand pre-payments*." (Manager).

On a similar theme, the Manager expresses that credit risks are also apparent in the industry, and in more high-risk countries, the risk can be mitigated by making use of letters of credit. It is explained by the Manager that "*Our treasury department performs a risk-analysis of new customers and suppliers where a demand is set towards the Delta sales-team of what we need to see*".

In regard to foreign exchange, the firm has made a deliberate call to move away from active currency hedging and instead now focus on a more natural hedge between the operational currencies. The Manager explained that whilst most large firms have these actively managed currency hedges, that it "*…is not completely risk-free either. You have to do it correctly. You need to secure both in- and outflows as soon as you get a new contract*". The company now instead relies on the natural hedging by maintaining a balance in the operational in- and outflows in the traded currencies. A major bank is consulted to perform an analysis on the basket of currencies they hold and if any measures have to be taken against potential risks arising from this.

4.1.4. Operational and strategic risks

In regard to the specific projects, the Manager explains that "*I do not believe that any risk simulations are conducted … but you do this bottom-up calculation, which becomes a sort of commitment from the sales side that: we need to achieve this*", meaning that the inputs of the sales team become very significant. These commitments are thus considered by Delta to be secure enough to trust that no other simulations are needed. Their sales commitment is placed within the firm's P-Calc, which together with other risk parameters and risk premiums adjust the bid, and are felt to be secure enough.

When asked about ERM frameworks specifically, both the CFO and the Manager explain that they do not use any external ERM framework, such as COSO (2017) or ISO 31000:2018 but that they use ERM. The CFO explains;

> "*We use the ERM-model, and we use it on a managerial level. In the risks we identify we take out an action plan. You usually identify the 10 largest risks, whereafter they are placed in order of significance, and strategic risk comes at the top. If for example we have one supplier, we give one person the responsibility to find more suppliers. We work in accordance with ERM, identifying large risks, but also doing something about them, like dual-sourcing in this case"* (CFO).

Since the respondents do not use any external framework, the question was raised regarding whether or not an internal framework with a formally stipulated risk appetite was followed or used, the CFO explains that "*No, ERM is a standard framework that I have worked with*" and the example regarding dual-sourcing is taken up once again. On the same question, the Manager explains further that "*No, but there is a regulation in regard to the bidding process, and which currencies are preferred and which currencies are no-go's without approval from the CFO*."

A common theme throughout the interviews is the respondents referral to the firm's Delegation of Authority (DoA). The DoA is a codified document which according to the respondents is a highly detailed and extensive document, stipulating what decisions managers and employees are allowed to execute within their domain of authority.

4.2 Managerial influence

4.2.1 Managerial risk perception and strategic judgement

When the question arose surrounding which formal tools or indicators Delta uses to measure risk, the CFO explains that;

> "*A lot of it comes down to a feeling based on what's happening in the world. For example, we want to move imports from China to the US, but a lot of the strategic level decisions are made on more or less a gut-feeling in regard to global events. We do however use bank analyses which daily provide us at Delta a look into what happens in the world*" (CFO).

Furthermore, these external measurements are also taken into consideration in strategic decisions, and together with the "gut feeling" constitute what becomes an implementation plan on risk, which the CEO then presents to the board, on which he receives feedback on what should be taken more into account. In regard to foreign exchange, Delta also use bank analysis' to forecast currency fluctuations, and only when the bank analyses and the managerial opinions differ, some kind of action is taken in the calculations of the P-Calc, which often constitutes an added risk premium or a "middle of the road" approach to the currency. The CFO explains further that;

> "*When you have more experience, you can take on more risk, but there is a tradeoff between risk and reward. Completely risk-free projects come with very low margins, and with higher risk you get higher margins as the risk taking is baked into the pricing towards the customers.*" (CFO).

This resonates with Mikes (2009, p. 22) notion that "a particular calculative culture both influences and is influenced by senior managers' choice and use of analytical models". The quotes show us a clear-cut example of when this is the case, and how the manager's inherent personal philosophies play a large role in the risk implementation plan. This resemble the situation in Delta, where the managerial feelings on macroeconomic outlooks, based both on bank analyses but also on gut feelings, could arguably reflect Grant and Nilsson's (2020, p. 2) notion on how decisions are based "on a myriad of factors and data concretized into rough estimates".

There are also clear similarities in the way Delta handles their risk ownership, with Ittner and Oyons' (2020) article, where multiple managers and their intuition work as limiting factors towards biases. One could argue that this way of having multiple managers work on this implementation plan with collective expertise, only for it to go further up the chain to the board of directors who ultimately through their expertise place a final judgement on it, works exactly as an internal control to limit any personal biases. But this also raises the question of where the expertise comes from, is there a possibility of groupthink for the levels in this modus operandi?

To further explore how differences in managerial philosophies play a role in the approach to risk management, we asked the CFO to explain to us if he felt there were any philosophy differences within the firm, or on a divisional level, to which he replied;

> "*All people have different viewpoints, the sales team for example want to sell more and therefore take on greater risks, so we have to have levels to regulate this. This is something that can be found in our DoA where the sales manager or someone above puts a stop to it before it goes too far.*" (CFO).

The CFO's personal view on the differences in risk management across the firm, thus seems to be based on conflicts of interests rather than differing managerial philosophies or expertise, and the mitigation of this is a strong internal control in the form of the DoA. When asked about evaluating factors and how the CFO personally evaluates a certain risk and if it has been handled correctly and with enough diligence, the CFO explains that

> "*You have to look at what to do to mitigate it, for example credit risks in China or late payments. This is handled in the calculation* (P-Calc) *and if it is as it is in China for example, where we mostly get paid, but it can take up to a year, we add a risk premium to reflect the lengthened payment horizon*." (CFO).

On the same note he adds;

> "*Technical risks become more and more common, where certain geographical customers can be quite difficult to handle, which makes you book more hours for engineering to make the design for the products, already in the calculation.* (P-Calc)" (CFO).

This addition of hours based on previous experiences, such as in the example regarding China or the technical risks, insinuates that the way to evaluate whether or not a risk has been thoroughly evaluated, rests almost solely on the gut instinct, and expertise which has arisen from industry knowledge, of the managers tasked with risk management. This is in direct opposition with Lundqvist's (2014) concept of full implementation of ERM based on the four pillars, which essentially states that in order to have fully implemented ERM in a firm, the firm among others, has to have a formal statement of risk appetite, as well as having alternative risk responses for each significant event. In Delta, as we have touched upon earlier, there are no formal statements of risk appetite, and instead of having a structure to find and mitigate risks,

managers find and evaluate the risks on their own, without much support from anything other than just previous experience.

4.2.2 Managerial influence on internal control systems for risk mitigation

The role of intuition and expertise in Delta's risk management can further be noted in the lack of formal mandate delegated to the Manager. He describes having significant influence on major projects, stating that the CFO and CEO are being "*Very responsive, I can provide very qualitative input and especially with the history that I have in the industry in different roles. So I have a very free role at Delta*" (Manager). The freedom of professional practice delegated to the Manager allows him to leverage his industry knowledge in order to focus on what he deems is important. The Manager put it the following way:

> "*The CFO doesn't really give me much guidelines, it's more like: go and do it and focus on what you think is important. And then if I think, for example, the P-Calc process is not functioning like it should – that I identify risks and shortcomings – then I have free hands to look closer at it and provide suggestions to the CFO*" (Manager).

Although the Manager states that he himself does not have any formal mandate stipulated in the DoA, the notion of his informal mandate to influence the ways Delta manages risks can be connected to the findings of Mikes (2009). One example of this can be observed in the Managers belief of how the management of currency risks could be improved:

> "*I also think with the currencies, that we need to change the approach that we have right now – we set up a kind of risk model in the quotation process that is [viewed] from an inflow perspective [...] and based on that define these risk commissions of what is needed to get a safe picture. [...] [but] when we sell in SEK, we always have different currencies on the outflow side, so it's not completely risk-free. [...] This is something I have talked with the CFO and Treasury Department about*" (Manager).

This quote highlights how the Manager influences and potentially co-creates the personal risk philosophies of those with formally stipulated mandates, in this case the CFO and treasury department. In the long run, this might entail him having an influence on Delta's calculative culture as described by Mikes (2009), by which his influence on their risk management

discipline is exerted through a judgmental risk assessment. This also aligns with the findings of Hall et al. (2015), who portray managers as tool makers in the process of improving risk mitigating practices. The Manager's involvement in the process of how Delta interprets and addresses currency risk, may suggest that the process of ERM is less of a static process, and more so a dynamic and co-created process.

Moreover, the interpretative prerogative delegated by the CFO to the Manager might not be emerging purely due to his industry expertise. The participative role he assumes might function as an incentive as highlighted by Malmi et al. (2020). Through the lens of agency theory, if effectively implemented, incentives like these would enable the principals of Delta (i.e. the board, or in this case the CFO) to align interests at a lower agency-cost (Jensen and Meckling, 1976).

These findings highlight how an informal mandate may serve as a subtle, but important part of an organization's risk management system. The durability of Delta's ERM practices thus appears to be contingent on cultural and interpersonal dynamics that shape them over time, raising the question of what happens if leadership changes?

4.2.3 Managerial interpretation of ERM and its influence on risk management

The reliance on informal trust-based systems in Delta has an important part in sustaining the risk practices that we have observed. Both respondents also seem to think that it works without that many hiccups. However, this reliance also reveals a fragility, a concern, as when individuals act as the judgement callers, the functionality of the system depends more on people than principles. This concern becomes even more clear when taking a look at the understanding, or misunderstanding, of ERM at a managerial level.

When questioned regarding whether or not external frameworks for ERM were applied in the firm, the CFO explained, as previously mentioned in section 4.1.4, that "*No, ERM is a standard framework that I have worked with.*", potentially showcasing that the understanding of ERM in Delta, appears limited in its scope. Delta appears to be focusing on a slim area of ERM and neglecting the larger image, which includes broader strategic dimensions as mentioned in for example Lundqvist's (2014) article.

Even though the overarching knowledge on the full implementation of ERM within the firm, is limited, the CFO in particular plays a very important role in assessing and mitigating risks in practice, as a part of his direct responsibility is to make sure that there is alignment with the firm's strategic goals, for example in overseeing the offering process. The CFO explains further that "*It is important that the risk is assessed by those who have the competency to do so*." with a further explanation that this is all stipulated within the DoA. The risks are in other words not handled in a systemic way, but rather, as we have already covered, in an interpretative and collective process which is permeated by industry and personal experience, as well as interpersonal trust.

One could argue that the CFO's understanding of ERM influences how risk is acted upon in the organization, as rather than being assessed against a formalized risk appetite, or quantitative thresholds and measurements, decisions rely heavily on expertise which comes from an accumulated experience within the industry. This open and collaborative culture of assessing risks gives a collective possibility for what the Manager calls "*pulling the handbrake*" when something seems too risky. This behavioral concept of using expertise as a way to make decisions, closely aligns with descriptions of Fingerspitzengefühl from Grant and Nilsson (2020).

4.3 Risk ownership and the limits of delegation

When asked about the DoA-document's structure, the Manager described it the following way:

> *"Here at Delta, we use an Excel-based model, which is available as a standard document in our process management tool, that anyone who needs it can access. It is essentially an activity-based matrix, built around a RACI[2] model, that clearly defines roles and responsibilities.* [...] *It is divided into different functional areas, everything from IT, procurement, representation fees, material disposal, and new hires. It's a highly detailed and comprehensive document, which is typically what you see in larger organizations."* (Manager).

[2] RACI: A format of responsibility assignment stipulating what organizational roles or players are responsible, accountable, consulted, and informed in a project (Project Management Institute, 2004).

This structure is confirmed by the CFO, stating that "*The Authorization matrix, or DoA, defines who is allowed to approve what. Is it, for example, a currency risk of larger character, it is raised to CFO-level to either be approved or to be sent back for revision*". This notion of risk treatment being embedded in the DoA emphasises its broad reach within the organization. "*Quotes [to customers] can involve many risks, looking at our largest product category, it starts with strategic risks, technical risks, country-specific risks, all of which are managed according to an authorization matrix*" (CFO). The Manager also noted how there is "*a decision matrix one has to follow in order to get approval from the person that has mandate for that size and types of investments*" and that "*you have different supporting systems that support this, that you document the approval processes and have traceability, such that there are points of control*".

This codified system of authority can be interpreted as a part of Lundqvist's (2014) two first pillars for ERM, referring to the general internal environment and control activities. In this view it is apparent that Delta through their DoA have incorporated aspects that are providing a general foundation on which ERM can be built, particularly referring to formally defined responsibilities, monitoring of processes, as well as the review, documentation and verification of policies and procedures (Lundqvist, 2014).

Both respondents note how Delta tries to disperse decision-making as much as possible, with the CFO stating that "*you let the risks be managed as far down in the organization as possible*". When asking the Manager whether the CFO's notion imply that the DoA actively tries to delegate tasks as far down as possible, with managers acting as supervisors to ensure that authority is practiced within the stipulated framework, he confirms our understanding, emphasizing that "*a healthy organization, it [the delegation] works if you have approval at the correct level*" (Manager). The manager adds further by stating that:

> *"It is good that you give mandate to people closest to the information and the decisions, and perhaps if we are talking about projects that are in relation with the customers, you will get the best results if you drill down the mandate as far as possible without losing control."* (Manager).

Two examples help illustrate how risk ownership and decision-making unfold within Delta. The first concerns the origin of strategic initiatives, which typically begin at the business unit

level. However, as the Manager points out "*it could also be the supply chain, who may see a big advantage in insourcing or outsourcing*". When asked what this process looks like in practice, the Manager describes a structured escalation path through the organizational hierarchy. In response to how many hierarchical levels a decision typically passes through before reaching implementation, he explained "*That's how many levels you actually go through with the heaviest investments*". The decision-making hierarchy that governs this process is visualized in **Figure 1**.

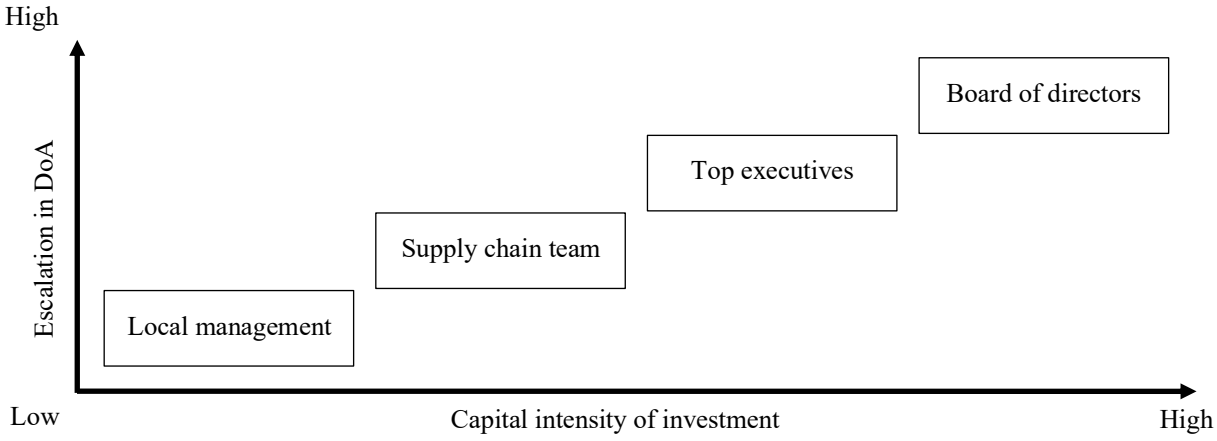

Figure 1: The hierarchical levels an investment must escalate within Delta's DoA, presented as a linear relationship by which a higher degree of capital intensity results in a higher hierarchical level of approval.

The second example concerns how responsibility is delegated to sales and engineering functions in the quotation process. Customer proposals are built using a modular concept, where standardized components are combined to meet the technical specifications required by the customers. Delta's engineering department develops the technical foundation for new products, which is then priced by the purchasing department using internal benchmarks and recent price data. As the Manager explains: "*It is like a price catalog where you select which products you want, setting a total cost by which other risk parameters are added on top*". The degree of product standardization further influences pricing as the model "is built from a discount perspective, so that if it is highly standardized it gets a certain discount on the price itself".

This process gives significant responsibility to those closest to the customers, aligning with the Manager's view that "*it is good that you give mandate to people closest to the information and*

the decisions". However, he also underscores the limitations of this system and in turn places responsibility on the sell side that the numbers are accurate from the start, stating that
"*I do not believe that any risk simulations are conducted – what happens if costs go up or something like that – but you do this bottom-up calculation, which becomes a sort of commitment from the sales side that: we need to achieve this*" (Manager).
These examples of how decision-making and risk management is delegated within Delta provides a nuanced interpretation of the existing ERM literature. Contrasting Lundqvist (2014), who emphasize that risks should be attended through a centralized department or staff function, Delta appears to have delegated risks broadly throughout the organization. Although Delta's delegation of authority aligns with Lundqvist's (2014) first pillar of ERM, the actual practice of pushing the practice of evaluating risk to the operational level complicates the picture. In particular, the sales division's reliance on their own intuition in absence of formal risk simulations, mirrors Mike's (2009) notion of how risks can be managed through expertise and interpretation. Whilst Mikes primarily associates such practices with risks rarely materializing, Delta applies this approach to routine tasks associated with ongoing risks, such as currency fluctuations, suggesting a broader use of intuitive risk management than previously theorized.

This practice is also reinforced by the Manager's belief that the best results are achieved when those closest to the decision hold the mandate of decision-making. At first glance, this bottom-up delegation resonates with Mike's (2009) observation that empowering business units can give rise to value-enhancing practices. However, Delta's lack of risk quantification disconnects this link as the basis for their evaluation is absent. In this sense, our findings at Delta invert the conclusion of Grant and Nilsson (2020). Their findings highlighted that an overload of data drove managers toward intuitive decisions based on expertise, whereas Delta's managers are driven toward intuition precisely because of its absence.

Whilst this decentralized risk ownership may foster responsiveness, it also raises important questions regarding consistency, oversight, and potential bias. Ittner and Oyon (2020) emphasize that assigning decision-making to senior risk owners can improve ERM functionality by reducing biases. In Delta's case however, the sales team's informal reliance on intuition, rather than structured, data-driver risk analysis, raises questions about whether these risk owners possess sufficient seniority for this to be the case. Thus, whilst Delta's approach may empower business units and individual teams, it may simultaneously open up the organization to behavioral risk. This brings us into the practical work of decision delegation

at Delta, where the tension between local judgement and opportunism can be further analyzed through the lens of agency theory.

When asked whether individuals had ever acted outside of their delegated authority, or if risk ownership had ever been unclear, the CFO was firm with his response. He stated that the DoA is "*deeply implemented within the organization and it is a requirement that it is used in everything related to quotes, payment terms, purchases etc.*". On the question of ambiguity in risk ownership, he noted that it is "*clearly defined in the DoA, for example currency exposure and [risks associated to] cash flow*".

The Manager partially agrees and offers a more nuanced view. Whilst agreeing on the clarity of formal structure, he recalls instances where the DoA has not been implemented as intended. He explained that profit margins, used to evaluate performance at divisional and team levels, are monitored on a monthly basis to detect deviations, suggesting that accountability is often enforced retrospectively. He added:

> *"There are no concrete cases like that [intentional deviations or misuse]. But it does open up the possibility that you can manipulate – when you have models like this [DoA] – for your own gain. So it's important that you have a strict line from the company regarding ethics and compliance."* (Manager).

Coherent with the Managers analysis, the delegation of risk and decision-making inevitably opens the door for principal-agent related concerns. Building upon the research by Mitnick (1975) and Jensen and Meckling (1976), there is the core assumption that parties entering a principal-agent contract will maximize their utility. In the scope of this section on how authority is delegated within the firm, it is reasonable to assume that the agents in this case, meaning those who have been delegated authority by top management, might choose to exploit the system. It is evident that Delta have applied Eisenhardt's (1989) utilization of information systems in order to monitor and detect deviant behavior of the agents, namely the DoA. Whilst the CFO gives the impression of strict adherence, the Manager notes that deviations may occur, and that models like these always can be manipulated for personal gain. The Manager's observation might thus reflect the broader challenge described by Perrow (1986) and Jensen and Mecklin (1976), although it remains inconclusive on whether Delta have not aimed for stricter surveillance due to monitoring costs or other reasons. Since monitoring is unattainable

at zero cost, the conclusion can be drawn that there exists a trade-off between reduced alignment and oversight costs within decentralized risk management.

4.4 Incentive structures and behavioral risk

In line with Eisenhardt's (1989) two paths of aligning principal-agent interests, Delta also uses outcome-based contracts for a limited subset of employees. These contracts rely on the assumption that outcomes can be both reliably measured and attributed, an assumption that is challenged in complex environments (Eisenhardt, 1989). At Delta, outcome-based contracts, referred to as bonus contracts, are primarily evaluated against three criteria:

> "*The bonus program within business units is based on order intake, or gross profit. In other words the margins [of the unit]. Second is what we refer to as operational results [later concluded to be EBITDA], and lastly we have sustainability targets. These are the three parameters that dictate the bonus for those with bonus contracts. Then it may also be more detailed, such as [the bonus contract being contingent on] overdue receivables or inventory turnover – it depends on the type of job you have"* (CFO).

According to the CFO, approximately 60 out of Delta's +1000 employees are on bonus-based contracts, thus these contracts are primarily reserved for top management and key employees. The decision of who is provided with a bonus-contract is at the discretion of the CFO, suggesting a centralized and potentially selective approach to incentivization.

Whilst these contracts encourage financial and sustainability performance, they do not explicitly incentivize risk reduction. When asked whether Delta provides any direct incentives aimed at managing or mitigating risks, both the CFO and Manager confirmed this is not the case. As the CFO stated, "*You are awarded a bonus depending on how the business is going. If you take too many risks, there will be deviations in the results, and then you will receive a smaller bonus*". Given that Delta employees are not incentivised to reduce risks, the question was asked on whether the misalignment between having risk ownership but no bonus-contract can result in these employees taking more risk than what Delta wishes, the CFO responded:

> "*No, as there will always be someone responsible for the risk above the employee. If it for example concerns sales, you have the head of sales controlling the amount of risk*

incurred. [...] Lower [hierarchical] levels manage minor tasks, and the higher it [the tasks] rises within the hierarchy, the larger the risks become" (CFO).

The Manager offered a more cautious view in his response, stating that "*since project leaders or sight managers are evaluated on gross sales rather than inventory turnover there is a risk for sub-optimization by which priority is given to dispatch deliveries if one has bought too much inventory*". The Manager also raised concerns of how the overall bonus structure might create opportunities for exploiting the system, particularly through the manipulation of the re-use discount in the quotation model:

> "*If the sales staff see that they are located quite high in relation to the target price then maybe one bluff's a little with it [re-use discount] … The biggest KPI for the sales team is order intake, and therefore it can be precisely these kinds of mandates and parameters that are sub optimized for one's own benefit.*" (Manager).

This concern directly reflects the classic agency problem, in which agents are assumed to act in their own self-interest rather than aligning with the interests of the principal (Eisenhardt, 1989; Jensen and Meckling, 1976). Furthermore, the case of potential bluffing within Delta's sales team can be seen as an operational variant of Healy's (1985) findings, where agents may manipulate performance related inputs, such as re-use parameters, rather than formal accounting procedures in order to influence perceived outcomes and maximize rewards. Importantly, these potential actions would be exercised within a monitoring system the CFO perceives as robust, paradoxically reflecting a form of moral hazard, potentially allowing agents to exploit managerial trust to conceal opportunistic behavior (Eisenhardt, 1989). Thus, whilst Delta has formal delegation structures and incentive contracts in place, they might be insufficient in curbing subtle openings for opportunism in the operational decisions and activities.

It should be noted that both respondents believe the sales team are the more prone to taking risk compared to other functional teams within Delta, however the Manager adds "*...You have extreme risks on the purchasing side as well. They have a really big mandate in choosing which supplier to go with, creating a huge risk for bribes and stuff like that.*" (CFO; Manager). He then adds that "*I definitely think that he [the purchasing manager] has some kind of bonus clauses in his contract. [...] I would guess that it is something related to inventory levels*".

Similarly to the risk of opportunistic behavior in the sales team, this also reflects the classical agency problem (Jensen and Meckling, 1976).

Conclusive from the Manager's responses is however that the most prominent risk of agency related problems is on the sell side, and that Delta due to this are looking at changing the re-use discount in order to mitigate this: "*We should probably change that concept and rather mirror it, so that depending on how much new development you have, the higher the risk factor becomes*". He also notes that the proposed solution is something that he is used to from previous roles, adding that "*And then I think it is healthy, having a risk premium when you have a lot of engineering. You usually underestimate almost everything – surprises appear that you didn't see coming*" (Manager).

4.4.1 Participation and cultural incentives

Beyond formal delegation and incentive-based contracts, the role of the Manager reflects a broader cultural notion of participatory influence. Although having no formal mandate under the DoA, he describes having significant influence on major projects, stating that the CFO and CEO are being "*Very responsive, I can provide very qualitative input and especially with the history that I have in the industry in different roles. So I have a very free role at Delta*" (Manager). This aligns with how participation in strategic and operational planning is culturally valued in Nordic and Germanic settings, and how it may act as a complement or even substitute of formalized incentives (Malmi et al., 2020). Although it is reasonable to assume that not all employees of Delta have the same level of influence as the Manager, he describes that "*If someone has good ideas [...] there's a huge drive at Delta and a desire to improve every day. [...] If you can clearly see that you have a good idea and can pitch it well – then we will implement it almost immediately*" (Manager).

This suggests that Delta may also be relying on culturally embedded participatory practices as an informal complement to the more formal approaches proposed by Eisenhardt (1989). However, it remains inconclusive to what extent participatory influence is accessible or effective at lower hierarchical levels, or if it is perceived consistently across the organization. Whilst the Manager experiences a high degree of responsiveness from senior leadership, it is possible that employees further down in the hierarchy may experience these dynamics differently. If such informal influence is unevenly distributed, participation could function as

a selectively applied incentive mechanism in the likes of bonus-based contracts. This raises the broader question about how principals navigate the trade-off between delegation and control in practice.

4.4.2 The delegation-control trade-off

Ultimately, the tension between delegating responsibility and controlling the outcome cannot be entirely resolved. As the Manager reflects "*The risk of cheating can't be eliminated 100%, but it is really important that you give a big mandate, and people usually grow with it too, and you get better drive in the organization.*", strongly aligning with Jensen and Meckling's (1976) notion of the ineffective nature of monitoring systems. The Manager also notes how top-down control risks generating inefficiency where you have to "*hunt down all your co-workers*", whereas responsibility and that "*you really have a drive from the individuals*" fosters stronger performance. He emphasizes that this however requires a work environment that is built on transparency and dialogue between managers and employees. The manager feels that this has been achieved at Delta, and informal conversations like these enable the development of a Fingerspitzengefühl allowing one to "*pull the handbrake if you feel that: No, this is too risky!*" (Manager). These insights emphasize that although formal structures such as the DoA and incentive systems are essential, the outcome is partly dependent on trust, corporate culture, and judgement. In practice, this highlights how Delta's perception of ERM is not only a formal exercise. Their deployment of formal monitoring and incentives also act as a signal for control and accountability, when actual oversight is limited. This symbolic dimension of ERM in Delta will be explored further in the following section.

4.5 Symbolism

Delta presents its risk management system as being both comprehensive and robust. The CFO emphasized that "*ERM is managed by top management, whereupon they identify risks which they later distribute to risk owners"* and adds that *"Every year they look at ERM and what risks there are on a strategic level"*. The Manager and the CFO also underscore the role of the DoA directing and dictating how Delta should approach daily operations, decisions, and risk management. The CFO considers the DoA to be deeply implemented and culturally respected within the organization.

This highlights that Delta uses many of the formalized systems presented by Lundqvist (2014) to be a prerequisite for functioning ERM. This includes Delta's use of bonus-contracts, monthly performance reviews, and clearly defined approval processes stipulated by the DoA. As the Manager notes, "*all approvals are documented and that there is traceability*", reinforcing the impression of a well-structured risk governance system.

Beneath these formal structures, signals of Delta applying ERM symbolically begin to emerge. When asked if Delta used any external ERM frameworks as guidance, the CFO insisted that "*No, ERM is a standard framework that I have worked with.*", despite being unaware of any external frameworks such as COSO (2017) or ISO 31000:2018. Together with the CFO's notion that no firm wide formal risk appetite is stipulated, this may indicate that the ERM-practices within Delta are in line with those accusing the framework of being symbolic and hollow (Power, 2009; Soin and Collier, 2013). This indication of symbolism is further strengthened by the Manager's admission that he is unaware of how the process of identifying the 10 largest risks is conducted, despite positioning himself as the right hand of the CFO:

> "*I don't actually know how they run that job and what risks they have identified. We're probably all in on it, more or less.*" (Manager).

4.5.1 Informal practices and interpersonal trust

Whilst Delta's risk management presents a structured façade, the daily handling of risk often relies on informal mechanisms. This is highlighted both through the Manager's notion that "*a sort of commitment from the sales side*" is required to reach pre-set margins in the absence of formal risk simulations, but also the use of gut feeling in the considerations of macroeconomic developments:

> "*A lot of it comes down to a feeling based on what's happening in the world. […] strategic level decisions are made on more or less a gut-feeling in regard to global events.*" (CFO).

> "*...we have also compared how accurate these financial institutions and banks really are in their forecasts regarding currencies? [...] it is kind of good enough to take the rates that prevail in the market at the time of planning.*" (Manager).

This reliance on managerial intuition in risk mitigation, rather than formal identification, quantification, and response, contrasts sharply with Lundqvist's (2014) criteria for what an organization should fulfill to be considered to have full ERM implementation. Although risks at Delta are often accounted for in the shape of risk premiums, the preventative measures mainly reside in informal discussions and the Manager's notion of "pulling the handbrake" when something feels too risky.

Not only does this point toward Delta being quantitative skeptics, as described by Mikes (2009), but it also points toward the employees intuition being the main tool in practically accounting for and mitigating risks (Hall et al., 2015). These insights thus suggest that Delta's ERM functions less through structural enforcement and more so through interpersonal trust. The CFO's notion of Delta implementing ERM and the DoA always being followed, stand in line with Power's (2009) notion of box-ticking, and raises the question of whether the decentralization of risk management might resemble a sort of blame avoidance through delegation (Hood, 2002).

4.5.3 Partial conclusion

Taken together, Delta's approach to ERM appears to reside on a dual foundation. The first considers the formal structures that present the appearance of control, the other those informal practices grounded in professional intuition and interpersonal trust. Whilst tools such as the DoA and documenting procedures create rigorous procedures, these are as Lundqvist (2014) describes, connected to the monitoring of internal activities and not ERM explicitly. The decentralized risk ownership, absence of a formally stated risk appetite, and lack of indicators aimed at emerging risks, strongly indicates that Delta can be considered not to have implemented ERM (Lundqvist, 2014). The tension between formal processes and intuitive decision making within Delta thus reflect a broader dynamic of symbolic compliance in the lines of Power (2009).

From the perspective of agency theory, this reveals a potential blind spot. The decentralization of risk mitigation practices and ownership without sufficient means of monitoring, as well as incentive systems that are relatively easy to manipulate, greatly increases the risk of opportunistic behavior among employees (Perrow, 1986; Jensen and Meckling, 1976). The question may also be raised as to whether this decentralization of risk induces blame avoidance

through delegation, although we deem the answer inconclusive within the frame of this study (Hood, 2002). Finally, the fact that “pulling the handbrake” seems to be the only measure by which Delta actively prevents risk (as opposed to merely pricing risk through a parameterization), suggests that it is trust, not control, underpinning the ERM logic within Delta.

5. Discussion

The following section seeks to interpret the broader scope of the empirical findings in light of the theoretical framework laid out in this study. The discussion is structured around two parts: First, we walk through the ambiguity and practical implementation of ERM outside of the financial sector. Second, we return to the role of managerial intuition as well as the use of informal practices in decentralized risk management. Together these themes offer insight into this study's contribution to existing literature on ERM and managerial influence.

5.1 Contextualizing ERM in non-financial firms

This study contributes to the body of research questioning the universality and practicality of standardized ERM frameworks such as COSO (2017) and ISO 31000:2018. In line with Lundqvist (2014), Delta becomes one example of the conceptual ambiguity surrounding ERM, not only in its implementation, but also in its interpretation. Our findings suggest that ERM in practice may depart from the structured and calculative vision promoted in dominant frameworks and previous research, regardless of whether quantitative parameters are used for direct directions or broader trend. In the case of Delta, the absence of quantitative risk measurements and formalized statements forces employees to manage risks based on socially embedded processes shaped by managerial expertise, highlighting one example of how actors within the organization might constitute tool makers of the risk management process (Hall et al., 2015).

The expressed use of ERM in Delta also resonates with the criticism of ERM that the framework may become symbolic in nature, serving as a “box-ticking” exercise to signal accountability rather than ensuring actual control (Power, 2009). Furthermore, whilst Delta claims to “use ERM”, our findings show that only antecedents, not defining practices, of ERM are in place (Lundqvist, 2014). This mirrors the concern of the frameworks ambiguity and

subsequent criticism, whilst showcasing that ERM might very well be used symbolically and obscuring potential risks, in this case agency-problem related behavior (Lundqvist, 2014; Braumann et al., 2024; Power, 2009; Eisenhardt, 1989; Perrow, 1986).

By focusing on a manufacturing firm, we respond to recent calls for more context-sensitive and industry-specific research and help address a perceived inadequacy within the domain (Fasihi et al., 2022; Mikes, 2009). Our findings highlight how firms in less calculative environments potentially might rely on intuition, platforms of communication, and managerial judgement in risk management, practices all of which are difficult to measure and quantify. In doing so, our study contributes to broadening the contextual lens through which the extent of ERM's understanding and implementation previously have been analyzed.

5.2 Managerial intuition and informal shaping of ERM

Our findings also contribute to the understanding of the role of interpretation and managerial intuition in risk management processes (Mikes, 2009; Hall et al., 2015). The case of Delta reveals how risk identification and response may rely on judgement based on experience rather than formalized simulations or quantitative forecasting. It highlights the instance of how managers could operate with autonomy to identify risks, relying on a "Fingerspitzengefühl" developed through long-going experience within the industry. Although it remains inconclusive of whether this applies to multiple managers within Delta, as well as managers and employees on lower hierarchical levels, our findings resonate with Hall et al.'s (2015) findings of managers as toolmakers in shaping risk management systems.

Particularly relevant in Delta is how the Manager, despite lacking a formal mandate under the DoA, actively participates in risk identification and construction of mitigating measures in relation to Delta's currency exposure and risk. This invitation for participation seems to be enabled through a cultural openness and trust-based delegation from senior leadership practiced parallel to the formal DoA, but raises important questions about the consistency and scalability of such delegations. More broadly, it taps into the notion by Malmi et al. (2020) on how delegation and participation might act as complement to traditional monitoring and incentives (Eisenhardt, 1989).

All indications point toward Delta's reliance on intuition not being a deliberate cultural strategy, but rather a compensatory response to the absence of detailed tools aimed at measuring current and emerging risks, suggesting that intuition may be as much a necessity as a preference. Whilst this absence undeniably introduces the potential of opportunism, the findings remain inconclusive as to whether these practices would persist under more formalized ERM structures or be replaced by data-driven processes, similar to the calculative cultures as proposed by Mikes (2009; 2011). This ambiguity does however add to the debate regarding the limits of formal control, both within the ERM, but also within agency theory (Mikes, 2009; Hall et al., 2015; Power, 2009; Perrow, 1986).

6. Conclusion

6.1 Summary and contributions

This study has examined how Delta, a multinational original equipment manufacturer, approaches enterprise risk management (ERM) in practice. Drawing on seven in-depth interviews with senior executives and guided by agency theory, the study explores how Delta identifies, delegates, and mitigates risk within a decentralized organizational structure. In doing so, we illustrate the tensions between formal control mechanisms and informal practices based on judgement, highlighting how symbolic and interpretive application of ERM may emerge in less calculative environments.

Our contribution to existent ERM literature is twofold. First, the study contributes to the debate on conceptual ambiguity and symbolic use of ERM by showing how risk may be formally addressed whilst informally managed through intuition-based practices. In particular, we show how risk management at Delta rests on managerial perception rather than quantifiable analysis, especially in day-to-day operations. Second, we contribute to research on managerial influence by highlighting how interpretative mandates, participation, and trust can complement and substitute formal control in the symbolic adoption of ERM. The findings suggest that in the absence of sophisticated quantitative tools, managerial intuition may act as a practical mechanism of risk mitigation, albeit potentially introducing agency-related problems and inconsistencies.

6.2 Limitations

Whilst this study provides meaningful contributions to literature on ERM and managerial participation, several limitations should be acknowledged. First, our findings are highly contingent on interpersonal relationships and cultural dynamics specific to Delta, which may not generalize to organizations where risk management is more formalized or quantifiable. Second, the seniority of the respondents constrained interview durations, which may have limited the depth of insights, where longer or additional interviews potentially could have enhanced data quality. Third, as with most qualitative studies our findings are susceptible to researcher bias, particularly given the interpretative nature of the analysis. Fourth, although the literature review draws on influential works following the 2007–2009 financial crisis, there remains a possibility that certain findings or theoretical models developed in these papers may be dated or less relevant in today's risk landscape. Finally, the study focuses largely on senior perspectives, leaving a gap in the understanding of how delegated risk ownership and managerial intuition play out at lower operational levels.

6.2 Suggestions for future research

Further research could build on several key insights from this study. First, we encourage further research into how managerial intuition and participation influences risk mitigating practices, particularly in environments where formal forecasting and simulations are lacking. Longitudinal or observational methods could offer a deeper understanding of how such intuition develops and whether it persists under shifting organizational structures or leadership. On a related note, research could also be conducted on participation as a potential substitute for formal incentive systems, particularly when risk ownership is delegated.

Second, future studies could examine the scalability and consistency of trust-based, informal delegation practices across organizational hierarchies. Given that our findings are context-dependent, comparative studies across firms and industries where numerical risk practices are less institutionalized, could help uncover whether Delta's model reflects a broader pattern or a unique case. Finally, echoing calls from Mikes (2009) and Fasihi et al. (2022), we reaffirm the need for more contextually sensitive studies of ERM implementation outside the financial sector, particularly in industrial and manufacturing environments where calculative risk infrastructures may be less developed.

7. References

Adams, M. B. (1994). Agency Theory and the Internal Audit. *Managerial Auditing Journal*, *9*(8), 8–12. https://doi.org/10.1108/02686909410071133

Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of Enterprise Risk Management. *Accounting, Organizations and Society*, *35*(7), 659–675. https://doi.org/10.1016/j.aos.2010.07.003

Bank for International Settlements. (2013). *The Basel Committee: A brief history*. https://www.bis.org/bcbs/history2_obsolete.htm

Bank for International Settlements. (2017). *Basel III: International regulatory framework for banks*. https://www.bis.org/bcbs/basel3.htm

Bonner, S. E., & Sprinkle, G. B. (2002). The effects of monetary incentives on effort and task performance: Theories, evidence, and a framework for research. *Accounting, Organizations and Society*, *27*(4), 303–345. https://doi.org/10.1016/S0361-3682(01)00052-6

Braumann, E. C., Hiebl, M. R. W., & Posch, A. (2024). Enterprise Risk Management as Part of the Organizational Control Package: Review and Implications for Management Accounting Research. *Journal of Management Accounting Research*, *36*(2), 7–29. https://doi.org/10.2308/JMAR-2021-071

Cooper, D. J., & Morgan, W. (2008). Case Study Research in Accounting. *Accounting Horizons*, *22*(2), 159–178. https://doi.org/10.2308/acch.2008.22.2.159

COSO. (2017, June). *Enterprise Risk Management: Integrating with Strategy and Performance*. Committee of Sponsoring Organizations of the Treadway Commission. https://www.coso.org/_files/ugd/3059fc_61ea5985b03c4293960642fdce408eaa.pdf

Eisenhardt, K. M. (1989). Agency Theory: An Assessment And Review. *Academy of Management. The Academy of Management Review*, *14*(1), 57.

Grant, M., & Nilsson, F. (2020). The production of strategic and financial rationales in capital investments: Judgments based on intuitive expertise. *The British Accounting Review*, *52*(3), 100861. https://doi.org/10.1016/j.bar.2019.100861

Hall, M., Mikes, A., & Millo, Y. (2015). How do risk managers become influential? A field study of toolmaking in two financial institutions. *Management Accounting Research*, *26*, 3–22. https://doi.org/10.1016/j.mar.2014.12.001

Healy, P. M. (1985). The effect of bonus schemes on accounting decisions. *Journal of Accounting and Economics*, *7*(1), 85–107. https://doi.org/10.1016/0165-4101(85)90029-1

Hood, C. (2002). The Risk Game and the Blame Game. *Government and Opposition*, *37*(1), 15–37.

ISO. (2018). *Risk management: ISO 31000*. *2018*.

Ittner, C. D., & Oyon, D. F. (2020). Risk Ownership, ERM Practices, and the Role of the Finance Function. *Journal of Management Accounting Research*, *32*(2), 159–182. https://doi.org/10.2308/jmar-52549

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, *3*(4), 305–360. Scopus. https://doi.org/10.1016/0304-405X(76)90026-X

Jordan, S., Jørgensen, L., & Mitterhofer, H. (2013). Performing risk and the project: Risk maps as mediating instruments. *Management Accounting Research*, *24*(2), 156–174. https://doi.org/10.1016/j.mar.2013.04.009

Lee, B., & Humphrey, C. (2006). More than a numbers game: Qualitative research in accounting. *Management Decision*, *44*(2), 180–197. https://doi.org/10.1108/00251740610650184

Lundqvist, S. A. (2014). An Exploratory Study of Enterprise Risk Management: Pillars of ERM. *Journal of Accounting, Auditing & Finance*, *29*(3), 393–429. https://doi.org/10.1177/0148558X14535780

Malmi, T., Bedford, D. S., Brühl, R., Dergård, J., Hoozée, S., Janschek, O., Willert, J., Ax, C., Bednarek, P., Gosselin, M., Hanzlick, M., Israelsen, P., Johanson, D., Johanson, T., Madsen, D. Ø., Rohde, C., Sandelin, M., Strömsten, T., & Toldbod, T. (2020). Culture and management control interdependence: An analysis of control choices that complement the delegation of authority in Western cultural regions. *Accounting, Organizations and Society*, *86*, 101116. https://doi.org/10.1016/j.aos.2020.101116

McKinsey & Company. (2023, October 23). *What is business risk?* McKinsey & Company. https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-business-risk#/

Mikes, A. (2009). Risk management and calculative cultures. *Management Accounting Research*, *20*(1), 18–40. https://doi.org/10.1016/j.mar.2008.10.005

Mikes, A. (2011). From counting risk to making risk count: Boundary-work in risk management. *Accounting, Organizations and Society*, *36*(4), 226–245. https://doi.org/10.1016/j.aos.2011.03.002

Mitnick, B. M. (1975). The Theory of Agency: The Policing "Paradox" and Regulatory Behavior. *Public Choice*, *24*, 27–42.

OECD. (2013). *Interconnected economies: Benefiting from global value chains.* OECD.

Perrow, C. (1986). Economic Theories of Organization. *Theory and Society*, *15*(1/2), 11–45.

Power, M. (2004). The risk management of everything. *The Journal of Risk Finance*, *5*(3), 58–65. https://doi.org/10.1108/eb023001

Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society*, *34*(6), 849–855. https://doi.org/10.1016/j.aos.2009.06.001

Project Management Institute. (2004). *A Guide To The Project Management Body Of Knowledge*. Project Management Institute, Inc.

Ross, S. A. (1973). The Economic Theory of Agency: The Principal's Problem. *The American Economic Review*, *63*(2), 134–139.

Shleifer, A., & Vishny, R. W. (1997). A survey of corporate governance. *Journal of Finance*, *52*(2), 737–783. Scopus. https://doi.org/10.1111/j.1540-6261.1997.tb04820.x

Soin, K., & Collier, P. (2013). Risk and risk management in management accounting and control. *Management Accounting Research*, *24*(2), 82–87. https://doi.org/10.1016/j.mar.2013.04.003

Srivastava, P., & Hopwood, N. (2009). A Practical Iterative Framework for Qualitative Data Analysis. *International Journal of Qualitative Methods*, *8*(1), 76–84. https://doi.org/10.1177/160940690900800107

Yin, R. K. (2009). Case study research: Design and methods. In *Case study research: Design and methods* (4. ed.). SAGE.

8. Appendix

Appendix 1: Conducted interviews

No.	Role	Duration	Date	Setting	Recorded
1	Manager	~51 min	2024-11-07	Teams	Yes
2	Manager	~20 min	2024-11-18	Teams	Yes
3	Manager	~31 min	2025-03-05	Teams	Yes
4	Manager	~30 min	2025-03-05	Teams	Yes
5	CFO	~38 min	2025-04-25	Teams	No
6	Manager	~36 min	2025-04-25	Teams	Yes
7	Manager	~30 min	2025-04-30	Teams	Yes

Appendix 2: Example of interview guide

Introductory questions

1. Do you consent to this interview being recorded?
2. Do you have any questions or anything you would like to add before we start?
3. Would you like to describe your role within the company and your areas of responsibilities?

Questions related to risk management

4. What are the most prominent risks your organization is facing?
5. How are risk responsibilities distributed in your organization?
6. What types of measurement tools or indicators do you use to measure risk?
7. Are there or have there been any initiatives that have called for responsibility for certain risk areas to be placed closer to the operational level? How has this worked in practice?
8. How do you ensure that someone is not taking risks that go *beyond* their mandate?
9. How do you ensure that someone is not taking risks that go *within* their mandate?
10. How would you personally evaluate a particular risk to assess whether it has been adequately managed?
11. How do you ensure that decisions that involve a certain amount of risk are in line with the company's strategic priorities?
12. Do you apply any type of external risk management framework?
13. What do you see as the biggest challenge for risk management in your organization?

Appendix 3: Use of generative AI

In accordance with the Stockholm School of Economics guidelines for students regarding generative AI (Artificial Intelligence) and thesis writing, an appendix must be attached outlining the use of generative AI or any other transformative technology. Outlined below is how AI and other technologies have been used in this thesis:

I. Microsoft Word has been used to create an outline for the interviews subject to transcription. They were later cross-referenced with potential recordings of the interviews in order to detect any misspellings or wrong formulations generated by the tool. Microsoft Word is compliant with GDPR, ensuring the confidentiality of the responses given in the interviews.

II. Version 4.0 of Chat GPT has occasionally been used for feedback on overall sentence flow and grammatical errors in order to improve readability. No AI-generation has been directly included in the thesis, and AI was not used in the academic analysis of our findings. This ensures that any work in the thesis reflects and remains our own independent academic work and efforts. Finally, reflecting upon the use of generative AI (Artificial Intelligence) and other transformative technologies has provided insights of how it may be used as a tool of support, but also its limitations in providing accurate translations of text.