Sensemaking Operational Risk Manager -
a qualitative study on how to become successful as an
operational risk manager in the Swedish financial sector

Master’s Thesis 30 credits
Department of Business Studies
Uppsala University
Spring Semester of 2019
Date of Submission: 2019-05-29

Rasmusson, Jens
Österlund, Joakim
Supervisor: Rad, Alexander
Table of Content

ACKNOWLEDGEMENTS .................................................................................................................. 3
ABSTRACT ..................................................................................................................................... 4
1 INTRODUCTION .......................................................................................................................... 5
  1.1 RESEARCH QUESTION ........................................................................................................... 6
2 FRAME OF REFERENCE ................................................................................................................. 7
  2.1 PERSPECTIVES LEADING TO THE SENSEMAKING RISK MANAGER ........................................ 7
  2.2 RISK CONTROLLERS IN THE FINANCIAL SECTOR ................................................................... 8
  2.3 ROLE OF RISK CONTROLLERS IN DECISION-MAKING & ORGANIZATIONAL CHANGE ..................... 11
  2.4 ROLE OF RISK CONTROLLERS IN SHAPING SYSTEMS & TECHNOLOGY ..................................... 13
  2.5 SUMMARY ............................................................................................................................... 16
3 RESEARCH METHOD ................................................................................................................... 18
  4.1 RESEARCH STRATEGY ............................................................................................................. 18
  4.2 DATA COLLECTION .................................................................................................................. 19
  4.3 DATA ANALYSIS ...................................................................................................................... 20
  4.4 ETHICAL & METHOD CONSIDERATION .................................................................................... 22
4 EMPIRICAL FINDINGS .................................................................................................................. 24
  5.1. RISK CONTROLLER AS INDEPENDENT FACILITATORS .............................................................. 24
    5.1.1 Humility & Soft Approach .................................................................................................... 24
    5.1.2 Facilitation of Risk Talk ...................................................................................................... 27
    5.1.3 Framing Knowledge ............................................................................................................. 28
  5.2. RISK CONTROLLERS AS ENGAGED TOOLMAKERS .................................................................... 29
    5.2.1 Creative Formalisation ........................................................................................................ 29
    5.2.2 Translating Knowledge ...................................................................................................... 31
  5.3. NON-FINANCIAL RISK CONTROLLERS .................................................................................... 32
    5.3.1 Quantifying Non-financial Data ............................................................................................ 33
    5.3.2 Hybrid Role ....................................................................................................................... 35
  5.6 SUMMARY ............................................................................................................................... 35
5 DISCUSSION ................................................................................................................................. 37
6 CONCLUSION ................................................................................................................................. 40
REFERENCES ..................................................................................................................................... 42
APPENDIX ......................................................................................................................................... 45

Table of Figures & Tables

Figure 1. Sensemaking Risk Controller Model ................................................................................ 16
Figure 2. Qualitative Content Analysis .......................................................................................... 21
Figure 3. Sensemaking Risk Controller Model with Categories ....................................................... 21

Table 1. List of Interviewees .......................................................................................................... 20
Table 2. Coding Example .............................................................................................................. 22
We want to show our gratitude to all our interviewees who provided their devotion and knowledge to ensure a sufficient empirical data collection for this thesis. We also would like to express our very great appreciation to our supervisor Alexander Rad for the valuable guidance and expertise during the planning and development of this research. We are also thankful to our opponents at Uppsala University for challenging the content of our thesis, and to friends and family members that assisted us by proofreading and advising us in the final stages of the process.

Uppsala, May 29, 2019

Jens Rasmusson Joakim Österlund
Abstract

Title: Sensemaking Operational Risk Manager - a qualitative study on how to become successful as an operational risk manager in the Swedish financial sector.

Course: 2FE840, Master’s Thesis, 30 ECTS
Authors: Jens Rasmusson, Joakim Österlund
Advisor: Alexander Rad
Date of Submission: May 29, 2019

This research sheds light on the nature of the role of the operational risk controller in the financial services industry. The focus is on understanding how operational risk controllers interact with different layers of the organisation and become influential with the business lines and senior management. Nine semi-structured interviews were conducted with operational risk controllers, and it was found that their work is becoming increasingly focused on managing people with a view to creating mutual understanding. To achieve this, operational risk controllers should work more as independent facilitators in their interactions with the first line and senior management, as engaged toolmakers when adapting and reconfiguring tools, and as non-financial risk controllers when attempting to enable business leaders to understand the magnitude of operational risks.

Key words:
I Introduction

In the spring of 2008, the world felt the full force of the financial crisis – the most severe since the great depression of the 1930s. In the light of the Lehman Brothers default, American International Group’s bailout and Merrill Lynch’s forced merger with the Bank of America the financial system revealed its true vulnerability. At the time, confidence in the system was lost, and credits previously considered low-risk investments were either worthless or difficult to value. Banks practically ceased lending, and the lack of new credit and the widespread uncertainty affected the economy as a whole, with severe outcomes. The financial crisis lead to stricter regulation that resulted in considerable attention being given to risk management in financial institutions. As a result, the financial crisis and the resulting regulation are important events for this research since they focused attention on risk management.

Risk management today is not only about sharing operational routines, but also about focusing on social aspects such as corporate social responsibility. Many of the risks are products of the organizational setting and therefore require different perspectives and new ways of being managed (Power, 2009). Moreover, risk management is complicated by a number of additional factors – for example, more complex products, automatization, increased international presence and connectivity, as well as the fact that organizations operate in a more uncertain environment due to cyberattacks, data security issues, and the risk of reputational damage.

The magnitude of the crisis proved how inadequate most risk management frameworks were and motivated considerable changes to risk management in financial institutions (Bessis, 2010). Regulators, practitioners, and academics have all contributed to the post-crisis understanding of what went wrong and given advice on how to prevent it from happening again. In a sense it is typical that it took a disaster to generate reform in improving the handling of risk. Power (2016) argues that this is reasonable, since the prevention of accidents lies at the core of risk management. Moreover, disasters, scandals, and accidents have always driven research in risk management, and thus, Power (2016) mentions how despite an increasing amount of literature insufficient attention is given to the non-post disaster work of organizational risk actors. It is somewhat of a paradox that so much attention and interest is given to studies that focus on explaining the causes of disasters. Therefore, this research seek to fill a gap in the literature by taking a different position from the vast majority of literature in the field by adapting a proactive approach to the study of risk management, and specifically the role of operational risk controllers. The focus will lie on their role in everyday organizational life and their influence on decision-making.

Previous literature has discussed the changing role of operational risk controllers (ORCs) and observed their increased relevance in corporate governance and firm-level decision making (Mikes, 2009, Kaplan & Mikes, 2016, Hall et al, 2015, Palermo, 2016). Risk management is arguably becoming less about ensuring compliance and traditional tasks such as aggregating the impact and likelihood of risks, and more about enabling a firm to make decisions in a situation of ambiguity by making sense of multiple layers of information (Esbensen, 2019).
Organisations are becoming more integrated and that risk management is something that is emphasised by different professional bodies - and risk controllers possess a multi-layered role that involve both control and strategic functions. The aim of this thesis is to understand the nature of the role of ORC’s within the financial sector. Research has revealed that the nature of this role has undergone several changes, both in terms of influence and type of work (Mikes, 2016; Hall et al., 2015). It has changed from being a sub-discipline that works alongside other functions such as the financial safety and information technology departments, to a role in which the risk controller has more influence in strategic considerations and power to change things (Mikes, 2009). This study adopts a qualitative research strategy in terms of which nine semi-structured interviews were conducted. It examines how risk controllers interact and influence other layers of the organization, what characteristics are important for success, and how tools are used by ORC’s to drive change in the organization. This thesis contributes to the theoretical understanding of the changing role of the risk controller and their increased relevance in firm level decisions and strategy (Mikes, 2016; Hall et al, 2015, Palermo, 2016); while also providing practical assistance to provide inspiration in everyday work and suggestions on an alternative way of doing things. It provides suggestions on how to think when adopting risk techniques or systems, and suggestions on the way risk controllers interact with the risk owners in the first line of defence.

Finally, the focus of this research is therefore directed towards understanding the qualities that an operational risk controller requires in order to be effective and successful in today’s financial environment. Rather than attempting to examine disasters in retrospect, this work seeks to understand the normal risk practices, what is being done from day to day, and what actors are involved.

1.1 Research Question

The purpose of this research is to gain an understanding of the nature of the role of the operational risk controller in the financial sector. This leads to the following research question and sub-questions:

- What qualities are important for operational risk controllers in the financial sector?
- How do operational risk controllers interact with and influence other layers of the organization?
- How are tools, systems and techniques reconfigured and adopted by operational risk controllers
2 Frame of reference

This chapter begins with an explanation about different perspectives of risk management leading up to a perspective of risk managers as sensemakers. Secondly, we go over how operational risk controllers operate within the financial sector. Thirdly, we review the literature on the role of risk managers in decision making and in shaping systems within the organisation. And finally, we introduce a theoretical framework based of the sensemaking risk manager.

2.1 Perspectives Leading to the Sensemaking Risk Manager

Risk management was originally a scientific approach to reduce risk in the United States insurance market during the 1950s. At that time, risk management was defined as a systemic way to protect revenues and resources against harm or damage (Hamilton, 1996). Thereafter, financial risk management emerged with a more quantitative approach to mitigate financial risk. Bernstein (1996) explains that the techno-scientific perspective, managed risks by assigning probabilities to unfavourable events. This assumed that historical data was the best predictor of future events. The techno-scientific perspective operated under the premise that risk management was about quantifying the likelihood and impact of events. Mitigating risks could be regarded as improving processes and standardizing controls to reduce the likelihood of undesirable events. However, the techno-scientific perspective has been widely criticised in the research field (see Power 2004; 2009; Hoopwood 2009). Taleb (2009), in particular, is regarded as one of the more critical proponents; he argues that quantitative risk models often fail when they are needed the most. He points out that black swans – unlikely events with significant impact – occur more frequently than expected and that quantitative risk models rarely detect the black swan in time.

It is submitted that Taleb’s (2009) reasoning about the failure of quantitative models demonstrates how risk can be seen as something unobjectively measurable and manageable. In the research field there are three main perspectives that challenge the assumptions of the techno-scientific perspective, namely the (1) cognitive, (2) constructionist, and (3) sociocultural perspectives. These perspectives revolve around various ideas that underlie today’s risk management (Esbensen, 2019).

Thaler’s (2015) research explains in general how the cognitive perspective recognizes the irrational behaviour of individuals when they satisfy their self-interest. From this perspective, risk management is a product of our cultural and social interactions and should be understood as a guide for our choices about threats and opportunities. Risk assessment and measurement are more about ensuring that our perception of the social and physical world is not limited by our perception. The constructionist perspective argues that risk should be viewed as something subjective which is constructed. This implies that our perception of risk is influenced by our social and physical environment, but also by our experience and knowledge about how the
world works and whether we find the information reliable (Mikes, 2011). According to Palermo et al. (2017), the sociocultural perspective views risk as incalculable and as something that cannot be discovered by natural science, created or observed through our perception of what is relevant. Risk differs between social groups and can lead to disputes over control and blame for its creation.

Modern developments in the area of risk management have been formed by a combination of the above perspectives. The financial firm’s environment has become increasingly interconnected and risky. In response to more complexity, risk management has developed comprehensive risk management systems to deal with risk between multiple risk categories and organisational levels. This development is commonly referred to as enterprise risk management (ERM), which is a conceptual framework that aims at focusing on risks that compromise the business as a whole (Power, 2009).

Esbensen (2019) argues that it is risk controllers who need to make sense of the social environment on behalf of the organisation. He calls this perspective sensemaking. According to this perspective, risk controllers try to identify exposure to risk by gathering inputs from multiple sources – both through their own experience and that of others. The difficulty with this way of working is emphasized by the cognitive perspective. Inputs will vary depending on the specific individual’s perception. Individuals in the organisation will not follow the same line of reasoning, and two individuals might not recognize the same risk exposure. Sensemaking implies that risk controllers need to rely on past and present experience to determine what makes sense in the future. Risk management as sensemaking is about enabling the organisation to make sense of information and make forward-looking predictions about the unknown, based on the available data.

This paper takes the perspective of risk controllers as sensemakers and will seek to understand the various ways they gather information and use their experience and others too form an understanding of the unknown. Through this perspective it is possible to focus on the everyday work of risk controllers and how they become successful in today’s business environment.

2.2 Risk Controllers in the Financial Sector

Most financial services firms have adopted the principles of enterprise risk management (ERM), but there is still only a partial understanding of the role of the operational risk controller (ORC) within the financial sector. Risk controllers have traditionally functioned as an oversight and control function whose role is to develop and communicate a methodology. Within the financial sector the Three lines of defence is the standard model to prevent risk and manage uncertainty (Chapelle, 2018). The first line includes the business frontline personnel who beyond their traditional tasks are responsible for risks associated with their daily tasks and are thus referred to as the risk owners. The third line consist of the internal auditors who independently and objectively consult the business in a less involved manner compared to the second line. Importantly, the second line is where the risk controllers operate, and in a sense, the ORC’s role could be defined as that of a supervisor who guides the way risks are managed.
by offering suggestions, educating, and training the business in the ways of the risk framework. ORCs do not manage risk or implement any of the proposed methods; rather, they should fulfill the following three roles. First, they define the risk appetite for the business and the board. Second, they monitor risk exposures and own the risk management framework. Third, they provide challenges on information and business decisions regarding risks. Importantly, in other sectors operational risk management is referred to only as risk management (ibid.).

The operational risk function is said to own the method of risk management and ORCs are responsible for identifying inefficient processes, products, or systems. As mentioned, they provide oversight and independent challenge, which means that they do not implement any policies that are aimed at upholding the organization’s risk appetite. Picket (2011) describes risk appetite as the “[…] amount of risk to which the organization is prepared to be exposed before it judges action to be necessary”.

In addition, the firm must also consider risk culture. Risk culture is reflected in the norms, attitudes and behavior within an organization which directs the way risks are managed. The appropriate risk appetite an organization identifies will inevitably stem from its risk culture. The risk appetite is proposed by the risk function and chief risk officer before it is accepted or rejected by the board. The risk appetite framework is central, since it dictates what constitutes unacceptable risks (ibid.).

Furthermore, the role of ORCs is becoming increasingly complex, which is related to the fact that organizations operate in more uncertain and complex environment. In relation to complexity in organizations Wahlström (2006, 2009) observes various conflicts that existed within banks and between departments due to different frames of references, which resulted in a different approach being adopted to the relevance of risk management and the associated regulations. The different ways of doing things created conflicting perceptions in departments, which affected the ability of risk controllers to influence other employees and decision-makers, and to manage change within organizations.

Decaux and Sarens (2015) observe the problems and limitations that arise from the information overload that occurs when various functions and risk experts work in silos. Decision-makers are faced with an endless stream of information about various risks, incidents, and suggestions based on different perspectives and motives. Spira and Page (2003) discuss the motives at the root of these different approaches, when different professional departments seek to gain influence. Risk controllers and internal auditors regard themselves as control experts, information technology (IT) departments oversee the information being made available, and marketing and human resources want to assume more strategic roles, while operational employees view certain processes as their field of expertise. The problem that inevitably arises is one of combining different perspectives and motives, since decision-makers need to decide what to do and what to focus on. Too much information makes it impossible to prioritise and make effective decisions.

Operational risk management include activities that (1) identify, (2) assess, (3) mitigate, and (4) monitor risk (Chapelle, 2018). These four actions constitute the main activities of any risk framework. Chapelle (2018) explains that risk identification and assessment involve both
quantifying large exposures and tail risks, as well as weaknesses and vulnerabilities inherent to the business. The risks are quantified based on their impact and likelihood. For example, scenario analysis sessions could include senior risk owners, members of the executive committees and the heads of business lines, and the sessions should revolve around major business threats associated with strategic objectives. These brainstorming sessions typically occur one to four times per year, depending on the current situation of the organization (ibid.). Meanwhile, a bottom-up approach focuses on inefficiencies; the most common techniques include incident reporting, process mapping, and interviews (ibid.). However, it can be problematic when organizations focus too much on small risks, such as manual errors and process risks, since the bigger picture is ignored. Incident reporting is another bottom-up instrument for identifying operational risks (ibid.). Wahlström (2006) suggests that one problem with incident reporting could be that employees may want to hide exposure to operational risk, as it could adversely affect them or their unit negatively. This can lead to employees being reluctant to report incidents, which in turn leads to deficiencies in the overall incident reporting.

Wahlström (2006) suggests that in banks where the norm is to hide incidents rather than report them leads to the management being unaware of the true risk exposure or the probability of risk exposures materializing. More recent studies have illustrated that solid incident data can be obtained on a consistent basis by working with the risk culture (Palermo, 2016). On a related note, Chernobai et al. (2007) address the issue of a lack of historical data on operational losses, which makes it difficult to develop robust models for managing operational risk. This can be explained by certain difficulties when developing an internal incident database. One difficulty is that extreme capital losses occur rarely and therefore there are relatively few such incidents (Chapelle, 2018). To overcome this problem, banks can include both internal and external data in order to supplement losses with near-misses and to use scenario analyses and stress tests (Chernobai et al., 2007). However, Bali and Allen (2007) argue that it is important to account for the size and business mix of the various banks included in the database when using and compiling external databases used for calculating exposure to operational risk for an individual bank.

The role of risk controllers is undergoing a substantial change, the role requires not only substantial knowledge and expertise within risk management, but also an understanding of the overall business. In other words, the role requires both knowledge of the regulatory demands to ensure compliance and social skills for people management. Peter Druckner once stated that “[...] culture eats strategy for breakfast”, which highlights the need for risk controllers to master the social and cultural aspects. In addition, it is common practice in most financial firms and corporate governance frameworks to ensure that the risk controllers are involved in the decision-making of strategic importance (Mikes, 2009). Moreover, risk controllers are meant to support the first line in their decision-making, which is done primarily by ensuring that they meet objectives within the risk appetite and consider risks in their everyday decision-making.
2.3 Role of Risk Controllers in Decision-Making & Organizational Change

Previous research has observed the changing role of risk managers in organizations (Hall et al, 2015; Mikes, 2008a, 2011; Power 2007). As mentioned, this paper focuses on the operational risk controllers which in any non-financial organization would be just a risk manager (Chapelle, 2018).

Originally, Mikes (2008a) categorized risk controllers as either business partners involved in planning and performance activities or as compliance champions that ensure compliance with regulatory requirements. Mikes (2008a) describes how financial firms are required to implement an ERM framework. The ERM framework defines risk management as a high-level strategic activity. The role of the risk controller as a business partner is to understand strategic uncertainties and communicate them to senior controllers and business lines. Mikes (2008a) questions how risk controllers balance their contradictory responsibility as either compliance champions or business partners; the notion here being that excessive focus on compliance will reduce the risk controllers’ influence in communicating strategic uncertainties, while too strong a focus on advising may make it harder to uphold policies and provide independent challenge.

The compliance champion focuses on regulatory requirements such as Sarbanes-Oxley Act (SOX) controls and on safeguarding both internal policies, as dictated by the risk framework, and external policies based on regulation. The risk management framework is seen as a policy outline that determines what risks need to be addressed and by whom. The compliance champion oversees the framework and ensures senior management that the correct processes and controls are in place. Power (2007) suggests that the essential distinction between various business partnering roles as either strategic advisors or strategic controllers will differ, given varying attitudes and reliance on numbers. Strategic advisors become influential with the board as a result of their experience on what can go wrong in a business. They make judgements on what can go wrong with a perspective that challenges the assumptions that underlie a particular strategy or way of doing things.

The strategic controller focuses on providing an aggregate view of financial risks and on integrating risk metrics and models into performance management and management control systems. Risk controllers ensure that risk metrics are reliable and used. They advise senior management primarily by promoting a risk-return point of view based on quantifiable data. Mikes (2008a) deals extensively with the conflict between oversight, independent challenge, and differences in the impact on decision-making based on the ways numbers and risk metrics are used. However, while she talks extensively about how decision-making is affected, she does not discuss what is perhaps the greatest challenge, i.e. the effect of behavior and the nature of an organization’s culture from the bottom-up.

Furthermore, Mikes (2009) suggests it makes sense to distinguish between risk controllers that work with either a culture of quantitative enthusiasm or one of scepticism. Quantitative enthusiasts manage risk by the numbers and assume that risk measures are capable of reflecting the economic reality. They prioritise improving the accuracy of their measurement and analytical models. By contrast, the sceptics are less trusting of numbers and regard risk metrics as trend indicators. Quantitative sceptics use risk controls as systems to challenge taken for
granted assumptions, or adopt a contrarian perspective. The sceptics rely more on common sense and experience in accordance with the sensemaking perspective (Esbensen, 2019).

Kaplan & Mikes (2016) conceptualize the role and influence of risk controllers in a similar but new light, based on the work of several case studies. They mention how many risk controllers operate either as independent overseers of controls or as business partners, in line with the previous discussion about the conflict between compliance and advisory responsibilities. Kaplan & Mikes (2016) observe two additional roles of risk management, namely the independent facilitator and the dual/hybrid role. These roles were conceptualized based on an analysis of several case studies where risk controllers had different ways of becoming influential in decisions – for example, by approving new projects such as the jet propulsion laboratory, where risk controllers challenged and approved all new projects. This worked efficiently due to the domain expertise of the risk management function that enabled risk controllers to challenge the engineers in a credible way. However, this approach is less likely to work in multi-layered organizations, since it is not possible to have all the required knowledge at one’s disposal. Mikes (2016) mentions that the formal inclusion of risk controllers in the decision-making process might not be the right approach if the risk controllers do not possess the necessary domain expertise. Rather, a more independent and facilitating role could be as effective in creating relevant risk management discussion and could provide an environment conducive to risk-based decision-making.

In the cases of Hydro One (Mikes, 2008b) and LEGO (Mikes & Hamel, 2012) risk controllers did not influence formal decision-making, but rather framed the discussion and set the agenda that enabled communication about risk across the organization. Risk controllers in this role need strong interpersonal and communication skills and less knowledge about specific domains of the business. Instead, they operate with a degree of humility to facilitate a discussion that leads to a subjective and qualitative analysis of strategic uncertainties, enabling business controllers to allocate resources and priorities between operational and strategic risk.

Mikes (2016) writes about “The Triumph of the Humble CRO” and followed two chief risk officers (CROs), who had limited formal authority and resources, over an extended period. The CROs successfully implemented an effective risk management framework by building informal networks within the organization. Mikes (2016) concludes that even without formal decision-making authority, risk controllers can become successful by, for example, mapping and quantifying risk exposures that support the line controllers, who are responsible for managing the risk. Mikes (2016) argues that the more formal and top-down approach to risk management, where risk controllers impose their views on the business, may be less effective than a humbler approach. This is because the facilitation of the knowledge of the business controllers inevitably triumphs.

Furthermore, Kaplan and Mikes (2016) discuss the dual or hybrid role, which was encountered primarily in the financial services cases examined in their research. In terms of the hybrid role the risk function distinguishes between independent and embedded risk controllers and solves the tension between demands for independent oversight and business partnering. The financial firms had groups working as compliance champions and independent overseers. At the same time, they introduced embedded risk controllers with domain expertise, which meant they could
work closely with the business line and advise on decisions. Interestingly, Chapelle (2018) mentions that it is common practice among many firms in the financial service industry to utilize business line coordinators that function as the one-and-a-half line of defence within the risk management framework. This raises the interesting question whether the introduction of coordinators is necessary to solve the tension referred to earlier.

In sum the findings of this section, suggest that it will require a degree of humility on the part of risk controllers to invite employees from various business units to rally around one common understanding of the different risks facing the enterprise. From this perspective it is important for risk controllers to empower risk talk in the business lines, thus assisting those who carry out and implement the risk framework (Mikes, 2016) Risk management is supposed to address future events which is not possible without subjective information that can be disagreed upon, what the future holds is unlikely imagined similarly by different actors and the answer will not come from a single actor but from an aggregation of multiple perspectives.

2.4 Role of Risk Controllers in Shaping Systems & Technology

Power (1999) discusses the move towards an audit society where risk management focuses more on actions that are measurable. Measurable actions leave evidence, which provides an opportunity to justify their contributions and value. There is, according to Power (1999), a conflict between trust and control. Financial firms are required to be cost-efficient, which is becoming increasingly challenging given the number of standards and level of scrutiny under which they tend to operate. In a way, cost efficiency makes it necessary to standardise, but it is problematic given the specific nature of many operational risks. Standardized processes and controls are not always a perfect fit. However, the controls are unlikely to be removed once they have been implemented. Instead, new controls are introduced to address the insufficiency of the standardised control. Power (2004; 2009) suggests that this leads risk workers to become box-checkers and calls for a democratization of risk management, where bureaucratic standards are cast aside in favour of more communication and cooperation that can facilitate engagement from the risk owners. Power (2004; 2009) criticises the quantitative approach and its prioritization, since it allows risk experts to increase their influence and status – primarily because numbers provide evidence of effectiveness. He also criticises the concept of a single aggregate measure for a firm’s risk appetite, since it enables the quantification of risk and making it auditable. A concretized approach is problematic, because it incentivizes bureaucratic box-checking rather than imagining alternative future scenarios in a critical way. Power (2009) emphasizes the importance of dialogue and communication that is separate from the formalised audit trail process.

Similarly, ERM frameworks often portray risk management as a formal process of risk identification, reporting, monitoring, and control. However, the fact that these are complex and multi-layered activities makes it important to work in a systematic way and creates a demand for risk tools, techniques, and systems. Several issues arise if operational risk management is treated as a standardized process. Palermo (2016) addresses several of these: How and when do people feel free to report on risks and speak up? What kinds of cultures and technologies enable
risk reporting and analysis? In his study, Palermo introduces the concept of *techno-culture*, which supposes an interdependence between control technologies and organizational culture and that notions of culture inevitably become visible in reporting and other managerial systems. Palermo mentions three aspects of techno-culture. First, organizations should encourage staff to speak up by, for example, not punishing mistakes that were not deliberately made. The author finds that this concept is hardwired into the organization if a good tone is set at the top and through supporting technologies of control that enable a non-punitive environment. Second, interaction with technology should be promoted. Third, Palermo (2016) talks about business partnering and the importance of having risk experts that are familiar with the business so that they are able to engage and facilitate change by building trust and increasing interactions between actors.

Similarly, Hall et al. (2015) discuss *toolmaking*, which is a process in which risk controllers adopt, reconfigure, and adjust tools such as risk maps, scenario sessions, and incident-reporting systems. Toolmaking plays a vital role in how risk controllers become influential with regard to decision-making. Hall et al. (2015) study two banks and find that there are significant differences in the ways risk controllers communicate and work with and around risk tools. Moreover, the authors identify two categories of toolmaking experts, namely *compliance experts* and *engaged toolmakers*. In their example, compliance experts are those who develop tools that are relevant to their own work and that of an external audience. These tools serve an important function in ensuring compliance with policies and regulations, but have limited influence on any strategic considerations or decisions. Moreover, the authors discuss how compliance experts fail to communicate their knowledge to the business line in a way that enables mutual understanding and acceptance (ibid.) There is often a gap between the tools and the way in which the line controllers run their operation.

By contrast, engaged toolmakers at Saxon bank were successful in implementing early warning systems, consolidated risk reports, and scenario analyses. The reason for this success lay in managerial input from the users and the fact that tools were regularly revised and kept up to date, based on input from the users. The most important factor is therefore to include and make use of the risk owners’ individual knowledge. The authors also observed how the risk controllers were still needed since they could take a step back and provide more comprehensive knowledge to the business lines and senior management. Engaged toolmakers are therefore able to demonstrate that their tools are relevant and valuable to the organisation, and that they possess the right type of expertise to translate the knowledge into a format that is digestible (ibid.). This ensures that they maintain their influence over decision-makers, since risk controllers are present in the framing and sensemaking of unknown factors of strategic importance.

Hall and Fernando (2016) discuss the conflict between trust and controls and find that there are tensions in the formalization of risk management. Therefore, risk frameworks and the identification of key risk indicators can lead to productive conversations that provides trust and assurance to decision-makers, but can also displace meaningful attention ensuring compliance in the organization. In their research, Hall and Fernando observe how matrices and templates are used to understand and document risks. They find that documenting risks in templates could
facilitate getting employees to think about risks in a structured way, particularly in relation to the identification of risks, their potential significance, and what mitigating procedures might be available. In addition, the researchers emphasize that visual aspects and boundaries in templates could assist in making sense of the possibilities of risk work. In other words, the layout and order of the template could help shape employees’ perceptions and thought processes in relation to risk. This line of reasoning with regard to the potential of visual templates to affect actors and action is consistent with Jordan et al. (2013) analysis of risk maps mentioned earlier. In the case of templates, however, the focus is on the recording and reporting of risks and not on facilitating discussion about risks between actors in the organization. Hall and Fernando (2016) conclude that excessive emphasis on risk formats can potentially limit and constrain discussions about risk in the organization.

Another interesting finding in Hall and Fernando’s (2016) research is how risk management can become more focused on its own codification in templates and indicators than on providing advice and decision-making support to front-line staff. This is consistent with Power (2007) who argues that risk management activities in organizations can become primarily focused on standardized procedures that are codified and thus more easily auditable in order to demonstrate sound risk management. When too much attention is directed to the codification process there is danger that codified information will be regarded as the only or most important knowledge that counts (Hall & Fernando, 2016). Expressed differently, the researchers suggest – somewhat paradoxically – that codifying and formalizing risk management has the potential to hinder risk management efforts by limiting opportunities for other types of risk management knowledge.

On a related note, Jordan et al. (2013) studied the concept of risk mapping and the administrative issues and challenges that parties encounter when engaging in risk mapping. They also examined the ways in which risk maps are used to facilitate organizational action. Risk mapping is a tool used by risk functions to graphically present risks in a matrix format, indicating the probability of risks occurring and their potential impact. The objective of risk mapping is to aid risk functions in ranking risks on the basis of how critical they are and how urgently intervention is required. The ranking of risks is often visually reinforced by means of traffic lights. The three traffic light colours represent different zones of acceptability. More specifically, the green light on the risk map indicates that the risk is considered acceptable and no action is required to mitigate it. An amber light represents an acceptable risk, but one with regard to which action should be taken if economically feasible. A red light indicates an unacceptable risk exposure. The authors suggest that risk maps – in contrast to written documents such as protocols, time schedules, or technical specifications – provide a comprehensive project image that can be understood immediately, even without knowing on what concrete information the map is based (ibid.). They conclude that the visual and non-calculative character of the risk map is unmatched among other interrelated practices used by risk functions (ibid.).
2.5 Summary

The literature regards sensemaking risk controllers as people who understand that their task involves a lot of uncertainty, due to the complexity of the information around them and the organisation in which they operate (Esbensen, 2019). There is simply no time to consider all the available information and therefore the sensemaker realises that it is more important for the organisation to focus on the unknown threats rather than on verifying that the known threats are being managed. Second, the risk controller’s role in decision-making is discussed on the basis of the observation by Mikes (2009) about the business partner and Power’s (2007) distinction between the strategic controller and adviser. Ultimately the conclusion is reached that decisions should be facilitated rather than imposed (Mikes, 2016, Kaplan & Mikes, 2016). Third, the quantitative role is discussed on the basis of the criticism of reliance on numbers (Power, 1999, 2004, 2009; Kaplan & Mikes, 2016) and Mikes’ (2011) study on how combining subjective judgements and hard numbers is an effective way of managing future events. Finally, the way risk controllers use tools and techniques is discussed on the basis of the conflict between trust and control that is inherent in any organizational culture (Hall & Fernando, 2016, Palermo, 2016) but also in terms of how risk controllers can become influential by creating engagement around the adaptation and reconfiguring of risk tools (Jordan et al., 2013; Hall et al., 2015). Based on the literature review the following model is proposed:

![Figure 1. Sensemaking Risk Controller Model](image)

The sensemaking risk controller focuses on making decisions under ambiguity and attempts to make sense of complex situations. Sensemaking is therefore about gaining an understanding in a complex situation where a decision is required despite the existing uncertainty. It is submitted that the sensemaking risk controller can be observed in three different settings and ways of working: first, as an independent facilitator who has the humility to understand the limitations of his or her own knowledge and the power to enable effective communication across the organisation (Mikes, 2016); second, as the engaged toolmaker who ensures that tools are created and adjusted based on the knowledge of the users, while maintaining influence over decision-makers by translating the knowledge (Hall et al, 2015); and third, as the non-financial
risk controller, whose role is about how the risk controller interprets information from multiple sources and thus help generate a view of the available information that is taken into consideration in strategic decisions. In general, our conception of a sensemaking risk controller is that of someone who understands the importance of organisational culture. The sensemaking risk controller uses both systems and social networks to gain more knowledge about strategic uncertainties and vulnerabilities and to communicate to and convince the risk owners that their perspective is the most relevant.
3 Research Method

This chapter explains the research methodology and methods implemented for this research. First, the research strategy is presented, followed by the epistemological and ontological position adopted. In addition, reference is made to the advantages and disadvantages of the research tools chosen. The following part discusses the sample size and strategy applied, which is followed by the data analysis methods used to code the collected empirical data. The chapter concludes with a discussion on the ethical considerations posed by the research methodology.

4.1 Research Strategy

A qualitative research strategy was chosen as the most suitable for this research, since the objective was to study the nature of the role of risk controllers (e.g. Mikes, 2016). The research examined new characteristics of the complex second-line role in the management of operational risks. The research problem was to identify characteristics of an ORC in today’s financial institutions. The management of operational risk is regarded as a social phenomenon shaped by social actors that are complex and interpret the same objective reality in different ways. How to manage operational risk can to some degree be abstract in nature and therefore be governed by factors that are non-tangible and difficult to measure. These could be social or cultural factors, for example. More specifically, they could be the social relationship between fellow workers in the different lines of defence or the overall risk culture in the organization. The social relationship and the risk culture are abstract in nature and difficult to measure by quantification. This reasoning is consistent with the sociocultural perspective on risk that was highlighted in the literature review. The sociocultural perspective views risk as incalculable and unable to be discovered by natural science (Palermo et al., 2017). The decision to make use of a qualitative research strategy meant ignoring the natural scientific model of quantification in the collection and analysis of data (Bryman & Bell 2015). A quantitative research strategy may have been appropriate if the purpose of this paper had been different – for example, identifying or quantifying operational risk in financial institutions.

This paper embraces interpretivism as epistemology. Bryman and Bell (2015) explain interpretivism as an alternative to the positivist approach, and concerned with the emphatic understanding of human action rather than the forces that act upon it. This means that the social reality is regarded as a social construct that is constantly shifting. This paper adopted a sensemaking perspective which argues with constructionism as an ontological position. Risk is not something objective that can be observed, but rather something that is subjectively agree upon within an organisation (Esbensen, 2019). Risk is from this point of view created by the social environment and objectively perceived differently depending on various motives and perspectives (Spira & Page, 2003).
Moreover, Hellström (2008) argues that the reality is continuously recreated by its participants, based on their specific intersubjective understanding of it. We seek to study the everyday work of a risk controller but do not pursue objectivity and generalizability (Slevitch, 2011). The role of risk controllers is not static; rather, it is in a constant state of revision. In other words, one is constantly questioning how the role is defined and therefore the social construct can be different, based on events during the time period in which they exist. This research does not explicitly study the changing role of risk controllers, although it could be argued that risk controllers today need to possess a different set of characteristics than before and it is thus of interest to get a snapshot interpretation of the current role the risk controllers possess.

It is important to be familiar with the shortcomings inherent in adopting a qualitative research strategy. Qualitative research cannot pursue objectivity or generalizability and has been accused of being too subjective, i.e. its findings rely too heavily on the researcher’s unsystematic view of what is significant and important (Bryman & Bell 2015). Another criticism of qualitative research is that the study is difficult to replicate, and there are problems of generalization, which in turn leads to a lack of transparency. These shortcomings of the qualitative research approach are acknowledged, and hence it is anticipated that another researcher’s investigation of the same issue, with the same research methodology, will find and present a version of the social reality that differs from this study. As will be examined in more detail later, this paper makes use of a predetermined coding scheme. This increases the transparency of the research with regard to how the data was coded and analysed. If use had been made of grounded theory, one could argue that this research would have been less transparent.

When following a qualitative research strategy, use is frequently made of an inductive approach with regard how theory is connected to observations or results (Bryman & Bell, 2015). This research adopts an inductive approach, which means the data was collected with a view to building a theory and contributing to existing theory.

4.2 Data Collection

The primary data for this research paper were collected through semi-structured interviews, which can be regarded as a combination of a structured and qualitative interview. Bryman and Bell (2015) explain that in a semi-structured interview the researcher has a list of specific topics to be addressed. The list of specific topics is called an interview guide. Although the researcher has such a list, the objective of the interview is that the interviewee should be encouraged to answer the questions with a great deal of leeway. Bryman (1988) suggests that the objective of qualitative research is to acquire a better understanding of a social phenomenon from the study participants’ perspective. For this reason, attention was given to how the interviewee frames and understands the issues and events connected to the research problem. Semi-structured interviews were selected as a data collection method for this research since it was clear how the data would be analysed prior to the interviews. In addition, this study was undertaken by two students and the semi-structured alternative was preferred in order to ensure a modicum of similarity with regard to interviewing styles (Bryman & Bell, 2015). However, one could argue that an unstructured or qualitative interview would also have been suitable of this research topic.
With an unstructured or qualitative interview, it is less likely that the interview would have been framed by the researcher’s presuppositions or expectations (ibid.).

The participants in this study were found through strategic sampling. Contact was made with a number of individuals working in risk functions and operational functions who were therefore relevant to the research topic. The sample consisted of nine participants. The participants were contacted via LinkedIn and sent an information letter regarding the objective of the study and the terms of their participation. These terms included guidelines from the Swedish Research Council. The size of the sample was felt to be appropriate. However, Hellström (2008) argues that sample size in qualitative research becomes to some extent irrelevant, since samples are evaluated based on their ability to provide important and rich information. In short, the sample is large enough when the social phenomenon can be understood. The degree of transferability is, however, based on the vividness of the descriptions (Guba & Lincoln, 1994; Sale et al., 2002).

Candidates were chosen based on three criteria: (1) that they worked for a firm operating in the Swedish financial sector, (2) that they belonged to the second line of defence, and (3) that their professional title was “risk controller”. All the participants were interviewed in person, with the exception of one interview that was held via Skype, as the interviewee was stationed in another city. The interviews took place at locations chosen by the participants, which varied from their offices to cafés. The benefit of letting the interviewee control the environment is that it ensures that he or she feels comfortable, which in theory should lead to richer and more informative answers (Bryman & Bell, 2015). All interviewees agreed to being recorded, and the material was transcribed. The various interviewees are presented in Table 1 below.

<table>
<thead>
<tr>
<th>Interviewee</th>
<th>Work Title</th>
<th>Date of Interview</th>
<th>Organisation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Operational Risk Controller</td>
<td>11/03/19</td>
<td>Financial Org. 1</td>
</tr>
<tr>
<td>2</td>
<td>Operational Risk Controller</td>
<td>05/04/19</td>
<td>Financial Org. 2</td>
</tr>
<tr>
<td>3</td>
<td>Head of Operational Risk</td>
<td>11/04/19</td>
<td>Financial Org. 3</td>
</tr>
<tr>
<td>4</td>
<td>Operational Risk Controller</td>
<td>17/04/19</td>
<td>Financial Org. 4</td>
</tr>
<tr>
<td>5</td>
<td>Senior Operational Risk Controller</td>
<td>17/04/19</td>
<td>Financial Org. 4</td>
</tr>
<tr>
<td>6</td>
<td>Operational Risk Controller</td>
<td>18/04/19</td>
<td>Financial Org. 5</td>
</tr>
<tr>
<td>7</td>
<td>Senior Operational Risk Controller</td>
<td>23/04/19</td>
<td>Financial Org. 6</td>
</tr>
<tr>
<td>8</td>
<td>Operational Risk Controller</td>
<td>08/05/19</td>
<td>Financial Org. 7</td>
</tr>
<tr>
<td>9</td>
<td>Operational Risk Controller</td>
<td>08/05/19</td>
<td>Financial Org. 7</td>
</tr>
</tbody>
</table>

4.3 Data Analysis

In analysing the collected empirical data, the process adopted by Graneheim and Lundman (2004) for qualitative content analysis was followed. According to these researchers, the process starts with identifying meaning units in the dataset, which are words, sentences or
paragraphs containing aspects related to each other in terms of content and context. In the following step, the meaning units are condensed, or shortened, while the core is persevered. These are referred to as condensed meaning units. The condensed meaning units are then labelled with codes. The codes can refer to parts of the interview that address a specific topic. The next step in the qualitative content analysis is the creation of categories, which refers to groups of content that share a commonality. Krippendorff (1980) argues that categories must be exhaustive and mutually exclusive. In this case, exhaustiveness means that no data related to the purpose of the study should be excluded due to lack of a suitable category. Mutual exclusivity refers to the fact that no data should fall between two categories, or fit into more than one category. Finally, the categories are linked to themes, which can be describe as a recurring regularity developed within categories. The process is summarized in Figure 3 below.

**Figure 2. Qualitative Content Analysis**

This study discusses whether risk controllers should be viewed as sensemaking risk controllers rather than control and risk experts. The following three themes from the literature were identified with a view to defining the sensemaking risk controller: (1) independent facilitator, (2) engaged toolmaker, and (3) non-financial risk controller. These themes, together with their corresponding categories, are presented in Figure 4 below.

**Figure 3. Sensemaking Risk Controller Model with Categories**
The various themes can be further condensed into categories, codes, condensed meaning units, and meaning units. Table 2 presents an example of how the empirical dataset was analysed. The coding example below starts with a quotation from the transcription. The quotation, or meaning unit, is then condensed into a shorter version that highlights the core meaning. In this case, the condensed meaning units are given two codes, namely collaboration and risk talk skills. The interviewee explains that he or she does not merely want to push for new regulation, but rather implement regulation on the basis of mutual understanding. To implement regulation with mutual understanding requires collaboration and risk talk skills. These codes are linked to the Humility & Soft Approach category, which constitutes part of the Independent Facilitator theme.

**Table 2. Coding Example**

<table>
<thead>
<tr>
<th>Meaning Unit</th>
<th>Condensed Meaning Unit</th>
<th>Code</th>
<th>Category</th>
<th>Theme</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>You do not want to go out and start by saying; this is a regulatory demand; you have to do it. It is better if you get there through a mutual understanding. (Interviewee 4)</strong></td>
<td><strong>You do not just want to push for regulatory demands, instead you want to implement regulation with mutual understanding.</strong></td>
<td><strong>Collaboration skills, Risk talk skills</strong></td>
<td><strong>Humility &amp; Soft Approach</strong></td>
<td><strong>Independent Facilitator</strong></td>
</tr>
</tbody>
</table>

### 4.4 Ethical & Method Consideration

In conducting this study, the participants were informed that their participation was voluntary, and no monetary or similar compensation was given in exchange for their participation. In addition, the participants were informed that they could withdraw from the study at any time, without having to provide any explanation. This information was outlined by the researcher before the interview. All participants in this study consented to participate in the study without undue influence or pressure. With a view to respecting the integrity of the participants and their employers, no names have been mentioned in the study. Before the interviews began, all participants agreed to the interviews being recorded. They were informed that the recorded material would not be used for commercial or any other non-scientific purposes.

Bryman and Bell (2015) argue that authenticity and trustworthiness are the most essential criteria for qualitative research. Authenticity has to do with how reliable a study is and whether it achieved its objective. Semi-structured interviews can enhance authenticity, if performed well, since follow-up questions enable clarification and reduce the interpretative work of the researcher. In addition, open questions reduce the risk of interview bias, since the risk of leading the interviewees towards specific answers is reduced. The interviews conducted in this study used open questions that were based on themes rather than direct questions.
However, the method adopted for this study opens up potential issues with replicability. If a similar study were to be conducted in the future, the results could differ significantly due to variations in both situations and circumstances. The way risk controllers are highly contingent on the specific organisation changes in accordance with both internal and external changes that the organisation is exposed to. The results of this study are based on the perceptions of risk controllers regarding their own everyday work and place within the organisation. Their perception should by no means be taken as a comprehensive and objective view, or generalised to any greater extent than reasonable. This means that other studies could compare and refer to the findings of our research only when similar methods are applied.

Trustworthiness is related to the transparency of our data collection and analysis. It is believed that sufficient time was allocated to follow-up questions, however there is always a risk that answers get misinterpreted. To limit the risk, all interview data were transcribed, and it was ensured that interviewees could be asked to clarify their answers if necessary. Moreover, a potential drawback of the study relates to the meagre sample size. However, it was recognised that a saturation point might have been reached, as multiple interviewees had similar responses. This was felt to be an indication that enough data had been collected. Finally, freedom from tendency refers to ensuring objectivity and ensuring that the research does not provide a biased or false picture of what reality looks like (ibid.). To ensure a freedom from tendency, the objectiveness of the study has been illustrated on the basis of the manner in which the subject has been discussed and analysed. There has been no intention to obtain any specific result, in our understanding of the role of risk controllers in the financial sector.
4 Empirical Findings

This section presents the empirical analysis, based on the model introduced at the end of the theoretical section. Figure 4 illustrates the thematic coding of the model. First, three categories of the sensemaking risk controller are described, i.e. the independent facilitator, the engaged toolmaker, and the non-financial risk controller. These three roles are then elaborated on based on themes derived from the empirical data.

5.1 Risk Controller as Independent Facilitators

Current corporate governance policies such as COSO-ERM recommend that the risk function should have a voice with senior management and an influence in firm-level strategic decisions (Chapelle, 2018). Kaplan & Mikes (2016) discuss how risk controllers should work more as an independent facilitator who focus on creating a suitable environment for risk-based decision-making through meaningful discussion among different perspectives and motives. As will be discussed the independent facilitator role demands more interpersonal and relational skills and less business knowledge, since risk controllers understand that it is the risk owners that possess the essential knowledge. Instead of advising the business on the basis of their own expertise and/or regulatory recommendations, risk controllers should try to enable a mutually understood overview to be reached among different business functions and senior controllers across the organisation.

5.1.1 Humility & Soft Approach

The quotation below describes a risk controller as someone whose main responsibility is not to identify specific business risk, but rather to identify limitations to the risk methodology from a risk-based perspective.

_We, as a second line of defence, do not have the responsibility to identify specific business risks. Our main responsibility is to, from a risk perspective, identify inefficient processes, inappropriate products, inadequate tools etc. that might lead to reduced capabilities to manage risks on an enterprise level._ (Interviewee7)

Risk controllers can be more involved in decisions by balancing the compliance and business partnering responsibilities, thus separating the role as an independent risk overseer from the role of working closely with the business line.
When I do not get them to introduce what I want, I book a meeting with them and sit next to them; personally, I am very pampering. (Interviewee 3)

The above quotation illustrates that to describe risk management work as objective would be far from reality, and that the supportive function often leads to direct involvement and cooperation with the first line. Many of the interview subjects were concerned about maintaining their independent and objective role towards the first line, to avoid becoming the ones implementing a process which they would ultimately have to test and challenge.

I am only supposed to challenge the information that comes from the first line; I cannot both implement the process and then challenge the inefficiency of that same process. (Interviewee 3)

When there is a willingness to change something in our risk appetite, a new project or business opportunity, we tend to get involved. (Interviewee 4)

According to the interviewees, a large part of the role of a risk controller is about assisting the first line. All risk owners are responsible for their own systems, processes, and products since they have the necessary knowledge and overview to evaluate the impact and decide on necessary action plans. Assisting the risk owners to manage risks satisfactorily was identified as a critical challenge by the interviewees. All interviewees mentioned the importance of working with the second line in a supportive manner, while not imposing on their way of doing things. Organizations suffer from time constraints, and risk is rarely prioritized among all the various things that need to be done. The challenge becomes about changing the way risk owners think and work with risk, which requires the risk controller to transfer their risk-based way of thinking.

It is about training and preparing the business enough to be self-sufficient and independent in their ability to implement the risk management framework. (Interviewee 9)

In the end, it is about changing the way people think about risk, the way of thinking about risk needs to sit in the walls – the risk function cannot be everywhere. (Interviewee 4)

As mentioned, risk management is more about dealing with people and changing the way they think and act; after all, it is always people that ensure that processes and controls are carried out and decide how things get done and what gets done. A self-sufficient first line postulates that they understand the value of risk management. Making them understand requires humility on the part of the risk controller and an understanding of different perspectives.
Changing someone’s mind necessitates an understanding of that individual’s perspective before another perspective can be introduced.

You do not want to go out to the first line and start by saying: this is a regulatory requirement you are forced to comply. It is better if we get there through mutual understanding of why we should do it and what value it adds. (Interviewee 7)

Successful second-line work requires that you understand and consider different perspectives before making a case for your own. (Interviewee 3)

By approaching the first line with a humble and curious mindset it is more likely that the risk function will be successful. Instead of trying to tell them what to do, it is regarded as more effective to start by trying to understand what they do and why. If control is missing it is not necessarily the case that the first line has ignored the risk; instead, they may not have the resources to check it, or it may even be inefficient or unnecessary to do so. Mikes (2016) points out that it is the job of the risk controller to bring together different functions and personnel from the business to share and produce a common understanding of the risks facing the enterprise.

Recently we have been focused on mapping out who the risk owners are, which means that we try to find the function that can remediate the problem instead of listening to all the screams for help out there. (Interviewee 4)

The problem of identifying what information to act upon and which risks to prioritize is challenging for many organizations. Each function will always think that its own risk is the most noteworthy and alarming; for example, IT will talk about data and cybersecurity, and the compliance function about upcoming regulation. As previously mentioned in relation to the empirical evidence, the role of risk controllers in decisions is more about ensuring that risk owners can make sense of all the information to gain enough understanding to prioritize and make decisions in a more future-oriented and holistic fashion (Esbensen, 2019).

Another aspect is that the risk controller can avoid being out of his or her depth in terms of pushing for something unnecessary; it is rather about going into the discussion with a humble mindset that acknowledges that the person being controlled has a perspective that the risk controller needs to understand. Even in cases where the risk controller feels particularly strongly about his or her case, or has some regulatory agency, it is better to remain humble and non-pushy since it is more likely to lead to changes in behaviour and norms.
5.1.2 Facilitation of Risk Talk

The independent facilitator role is about speaking a language to which people can relate, which requires both an understanding of the business and a simplification of the risk jargon. Mikes discusses the importance of speaking in a language that can facilitate engagement and communication, and coined the concept of “risk talk” (Mikes, 2016). In a sense, the evidence presented in this paper is in line with the argument of Mikes about using a language that resonates with the business, instead of trying to teach the business lines a new way of communicating (Mikes, 2016). Moreover, Chapelle (2018) mentions how the use of vulnerabilities and exposures is to be preferred in, for example, Risk and Control Self-Assessment (RCSA) sessions, since this enables business lines to use words and terms that they are used to.

To effectively get your message across it is necessary to communicate using a language that is relatable. (Interviewee 9)

It is a lot about keeping dialogue with the first line and from there try to establish a correct picture given all the information. The information you get is rarely quantitative and aggregated it is often qualitative and not likely to be comprehensive; the work demands that you can cooperate and understand each other using dialogue. (Interviewee 5)

The above quotation provides a good summary and is integral to explaining the role of risk controller as an independent facilitator. Organizations face a momentous amount of information and, as already mentioned, it is becoming increasingly crucial for different business units to have a complete understanding of how their strategic decisions can have a potentially harmful effect not only on themselves but also on the entire organization. This view is difficult to achieve, and it is unlikely that business controllers will prioritise to that extent – preferring instead to focus on making money. Thus, the risk controller’s role becomes to try and influence the risk owners to adopt a way of thinking about risks that takes the organization as a whole into account.

Many business lines regard risk management as something external to their everyday task, and as something that is added on as more of a bureaucratic drill. The new way of working with risk in the financial sector is forced upon the organizations through increased regulation. The findings of this study suggest that the challenge for risk controllers going forward will be to convey a point of view that makes the risk owners in each business unit understand the value and benefits that result from effective risk management. Moreover, engaging with the business in a humble yet confident manner, and using language to which the audience concerned can relate, is the best approach for the risk controller. Influencing ways of thinking is impossible if the business concerned regards risk processes as bureaucratic controls that take time away from the business (Power, 2007). In general, the problem is not that it is challenging to compose processes, but rather that implementation and achieving continuity can be very demanding for
an organization. There are always fires to extinguish, but one-time overhauls are not a long-term solution, and this is recognised by the interviewees as a significant challenge going forward.

5.1.3 Framing Knowledge

The interviewees did not perceive themselves as advisors; instead, they often mentioned the supportive function and how they would give recommendations in an independent and non-involved way. Objectivity is emphasized, since the risk controllers took issue with being involved in the implementation process, when they would ultimately have to oversee that same control or process.

All new projects or changes will run through and be assessed within our new RCSA process; we are responsible for the agenda and enable a good climate for proactive discussion. *(Interviewee 6)*

The facilitating nature of what risk controllers do was discussed earlier, and it seems that while risk controllers do not advise or tell anyone what to do, they still impact decisions by framing the environment where decisions are taken.

When we do scenario analysis, disagreements are not uncommon among business functions; for example, IT can have a perspective that the others do not agree is particularly alarming in this situation. We can step in and help them understand each other. *(Interviewee 8)*

Given the complexity of the information that is usually available – and the uncertainty that comes with new ventures and strategic decisions – the risk controller’s role becomes that of someone that assists the decision-makers in making sense of all the available information, and ensures that there is a methodology in place to make sense of all this information Decaux and Sarens (2015) suggest that there is an overload of information within an organisation where similar or the same risks are reported, multiple times in different ways, among various functions, regions and levels. Decaux and Sarens (2015) suggests a combined assurance framework where the focus is on gaining a more holistic view of the organisation. However, he points to the internal auditors as the profession best positioned to achieve it. We found that most of our interviewees held the perception that they were better positioned to work in a supportive manner and enable the risk owners to gain a more comprehensive view of the risks they faced.
Gaining a comprehensive view of risks can be very difficult in practice; however, we believe that each risk owner needs to strive to get to a point where they take responsibility for not only themselves but the entire organisation. (Interviewee 5)

The problem of sorting out what information to act upon and which risks to prioritize is challenging for many organizations. Each function will always think that its own risk is most noteworthy and alarming; for example, IT will talk about data and cybersecurity, and the compliance function about upcoming regulation. As previously mentioned in relation to the empirical evidence, the role of risk controllers in decisions is more about ensuring that the risk owners can make sense of all the information to gain enough understanding to prioritize and make decisions in a more future-oriented fashion.

5.2. Risk Controllers as Engaged Toolmakers

A significant part of introducing the risk methodology to the first line involves education and training on tools and techniques. Hall et al (2015) describe toolmaking as the process where risk controllers adopt, reconfigure, and adjust tools such as risk maps, risk assessment matrices, or the incident reporting system. This line of work is in a certain sense about formal integration of risk management with the business and performance management. Hall et al (2015) differentiate between different toolmaking characteristics and describe the engaged toolmaker as someone who successfully demonstrates the value and relevance of risk tools, and possesses the right type of expertise to translate knowledge about how to use and why to use risk tools. The engaged toolmaker is someone who manages the tension inherent in the codification and standardisation of risk management (Power, 2007), understands that culture and technology is inherently intertwined (Palermo, 2016), and is able to transfer knowledge to the risk owners through the use of toolmaking.

5.2.1 Creative Formalisation

A prominent discussion when it comes to formalizing risk management revolves around Power’s (1999, 2004, 2007, 2009) issue with the fact that risk procedures are becoming increasingly standardized and bureaucratic. Hall and Fernando (2016) discuss the issues with standardized procedures that take time and attention away from more meaningful discussions about risk. The first line are the experts, since they possess all the knowledge about processes and vulnerabilities of a function.

A big challenge when introducing new ways of working is to get the business to put away time for risk management; they have another job, and this is something that is added to that. (Interviewee 2)
To some extent, it is more important that some incidents are mitigated and do not reoccur instead of all incidents being reported on and measured, since the focus should be on reducing costs. Trying to report everything would be detrimental to the organisation’s risk management, since there would be little actual dialogue and discussion about risk as the work would be too formalised (Hall and Fernando, 2016), regarded as overly bureaucratic (Power, 2007), or merely as something that would lead to more work (Palermo, 2016). Interestingly, the interviewees talked about combining quantitative data with qualitative data, such as trends or how they often quantified qualitative data, since the information rarely came readily quantified.

*It is important not to have too many metrics in place, especially if they do not measure something relevant. Moreover, if you have qualitative metrics, they need to be easy to monitor.* (Interviewee 2)

It is crucial to avoid becoming overly concerned with formalized processes to measure and quantify everything. Hall and Fernando (2016) mention how too many key risk indicators could displace the attention of an organisation to focus on codifying rather than discussing risk. Instead of measuring the number of incidents, the risk metrics could measure the trend of incidents being dealt with and mitigated. Several of the interviewees mentioned the importance of not building up too much bureaucracy and emphasized a desire to focus on advising and supporting the already time-constrained business lines. Hall and Fernando (2016) regard it as vital to prioritise, rather than merely codify procedures to make them auditable and demonstrable of sound risk management, while less actual discussion about risk is actually taking place.

*Tools and systems such as risk matrixes are useful, but the real work involves getting people to use them in the right way.* (Interviewee 1)

*When reporting on incidents, the first line often report that they were affected but did not quantify how much or specify how they were affected; in these situations, it is important to get in early and challenge the information.* (Interviewee 3)

Palermo (2016) discusses organizational culture and how it is worthwhile to work with supporting technologies that enable a non-punitive environment. Instead of trying to tell employees what to report and giving them guidelines on what to report, it is better to encourage them to interact with technology by removing any material criteria or demands and rather make them report everything in their own words. If it is difficult to make the first line report in a useful way, it is because they do not recognise the value of reporting, or may even be hesitant since it might lead to more controls or activities to contend with. When creating controls and systems for reporting, it is crucial to consider more than just formal requirements such as what
should be reported, and instead focus on ensuring the right organizational environment and incentives to report.

5.2.2 Translating Knowledge

Financial firms are advised to implement a risk management framework, and risk controllers often adopt tools based on recommendations from regulators. Compliance is central to any financial services firm, and adjusting tools to ensure compliance with policies and guidelines is important.

*External tools can be useful but without input from the risk owners it is hard to achieve what we want to achieve. There is nothing special about tools such as risk maps; what is special is the discussion they create.* (Interviewee 9)

The statement above illustrates how merely implementing the correct methods or systems is not enough to change things. It is not certain that the risk owner will continue to interact with the control in a way that mitigates the risk (Palermo, 2016). Within the second line of risk work, it is necessary to understand that risks are managed in the different business functions, which means that it is about changing behaviour and not only about imposing new controls and processes. Tools such as the risk matrix or risk plan and mitigation templates are meant to function in a supporting and educating manner, not as a means for the second line to ensure that policies and guidelines are followed. Moreover, Hall et al. (2015) mention how essential managerial input is to successful toolmaking, and that the best strategy is to reconfigure tools based on managerial input, on the key risks the risk owner regards as critical and on steps the risk owner would take to improve a product, process, or control.

*Even if nine out of ten IT systems are scanned for vulnerabilities, the last system might be the one holding 80% of the sensitive data.* (Interviewee 7)

It is unlikely that the risk controller will be the one who possesses the knowledge that certain IT systems hold most of the information. This knowledge is something that needs to be extracted from the first line, which obviously will not happen automatically. It is not guaranteed that the risk owner will continue to interact with the control in a way that mitigates the risk (Palermo, 2016). For risk controllers to manage risks effectively, it is necessary to understand that risks are managed in the different business functions and that promoting a healthy risk culture is essential for success.
Many see risk controls as something negative, but as long as they understand the value of reporting, I feel comfortable that they will report everything they perceive as relevant. (Interviewee 3)

Another aspect of the role is to achieve a long-term improvement where new processes are continuously maintained, since ensuring a successful implementation can be challenging. Several of the interviewees mentioned that it is challenging to ensure that improvements and changes to processes and controls are managed continuously by the business lines that are the risk owners.

To get all the processes to function every year is incredibly challenging, you want to avoid one-time overhauls that do not create any long-term change. (Interviewee 7)

ORC’s need to be aware that even when a control or process is in place, it may not even measure or identify what it is intended to. It is essential that controls make sense and function the way they are intended to, and that they measure the right things. However, how well tools are adapted and adjusted to fit the business becomes irrelevant if the people using them do not understand how or why these tools are used. While the interviewees in general emphasise the knowledge of the risk owner, their inclusion in decisions related to what tools to implement and how to form new controls seems to be limited. Our interpretation is that there may be a fear of transferring too much knowledge, and that this fear should be replaced by a realisation that the risk controller’s role is to enable the risk owners to improve on the tools and reconfigure them to fit their specific needs, while also translating external perspectives and more comprehensive knowledge into something that is digestible and considered by the risk owners.

In summary, the results indicate that the focus is on creating systems, tools, and techniques in a manner that can promote discussion and engage the first line in a risk-based way of thinking and behaving. The focus is therefore on organizational culture, and the function of tools is to support this culture (Palermo, 2016). Moreover, making the first line understand through the use of tools often involved quantifying and illustrating the financial impact, or potential impact, of incidents. Instances related to near misses, IT, and indirect risks such as reputational risks, were emphasized as particularly problematic.

5.3. Non-financial Risk Controllers

Quantifying constitutes a significant part of risk management, as it allows for the comparison of risk versus rewards, which is central to any decision. Furthermore, it is necessary to benchmark the firm’s aggregate risk exposure against its risk appetite. Operational risk controllers often work to provide an aggregate view of the financial risks facing the firm, to suggest risk metrics and to integrate them with performance metrics. The findings of this study demonstrate how risk controllers gather knowledge – both subjective and objective – from
multiple sources, and that the ability of the risk controller to communicate a comprehensive view is crucial for his involvement in strategic decision-making. This aspect of the role is therefore referred to as strategic interpretation, where the risk controller is supposed to function as an interpreter of strategic uncertainties for the business leader. This study has established that this has a lot to do with communicating non-financial risks, as well as the role of the strategic interpreter in resolving tensions regarding dual responsibilities through coordinators.

5.3.1 Quantifying Non-financial Data

The interviews made it clear that quantifying is an essential aspect of making people understand the value of risk management and the potential damage to operational risk, since they rarely have a direct financial impact. Moreover, it is rarely the case that different functions agree on what risks are essential, and they are likely to have different motives and perspectives on what to focus on (Spira & Page, 2003, Wahlström, 2006).

*Many have the attitude that if we do not have any losses, then there is no problem; salesman rarely want to blow up problems.* (Interviewee 3)

*It is essential to show the uncertainties and potential cost of a strategy or investment in the end; it is a lot about common sense.* (Interviewee 5)

Quantifying is a crucial aspect when it comes to increasing awareness of the potential consequences of strategic decisions. Unfortunately, it is a complicated task to quantify operational risks, and reducing operational risk always comes at a cost, since it requires investment. Moreover, risk-based decisions are something our interviewees emphasised when talking about strategic risks. However, the problem – as they saw it – was trying to promote the risk-based way of seeing things across the organisation, and that it unfortunately often requires a financial impact to make someone interested. Near misses or reputational damage due to loss of business are rarely seen directly, but rather as things that have an indirect financial impact (Chapelle, 2018).

*A lot of IT risks can be challenging to communicate, since few senior managers speak that language and there are rarely any hard numbers to showcase.* (Interviewee 3)

*I would like to shut down the server just to measure the amount of transactions that did not occur after the shutdown. Let’s say that 20% of the people that could not access the page during the shutdown did not go through with transaction; we then have a hard number; however, I am having trouble making this a reality with senior management.* (Interviewee 8)
IT issues rarely have a financial impact, yet there is a clear desire among operational risk controllers to showcase their indirect impact. Moreover, as is clear from the second statement, measuring indirect risks like this is rarely something that resonates with senior management. It is rarely a priority, but perhaps it should be. According to the data collected for this study, the risk controller has an important role to play in showcasing the indirect financial impact of these types of issues, and the work could start with finding a way to measure and quantify the risk and related financial impact.

As already mentioned, in a complex environment it is often not easy to decide what to focus on. Therefore, when it comes to operational risks, it is not easy to calculate which is a fundamental issue, given the notion that “what gets measured gets done.” The findings of this study indicate that some financial firms utilize four sources of information in their loss data estimations of operational risks. First, there is the internal loss data which ties a banks estimation to the actual losses. However, this usually only provides data on frequent incidents with insignificant effects, and thus underestimates the likelihood of infrequent incidents with a more severe impact. As Kaplan and Mikes (2016) point out, quantitative risk management should admit that there is a need for alternative quantitative models that utilize multiple data sources.

When estimating operational risk, it is the risk owners that bring the knowledge on scenarios and such; and then there are quantitative people assisting with probabilities and their estimates; we are rather passive unless something is missing or dysfunctional. (Interviewee 9).

Our estimations of operational risk loss data are derived from multiple sources and combined with scenario analysis and data from our internal control and external business environment. However, we are not involved with this estimation; we only provide means for this process to occur and give our input when necessary. (Interviewee, 8)

Moreover, scenario analysis based on experts from different areas is the favoured and essential method for assessing tail-risks. In addition, the larger firms that were part of ORX also made use of external data on operational risks to evaluate exposures, thereby assisting in estimating likelihoods and impacts of conceivable scenarios. The risk function plays a vital role in these estimations as a facilitator of the meetings and/or RCSA activities. Moreover, the risk function brings a risk-based perspective to the discussion and often has a complete picture and perspective that it can use to its advantage. The risk function understands the business environment with its emerging risks and internal control issues, and it is crucial that this perspective be transferred to decision-makers, since it makes the risk assessment more forward-looking and based on common sense.
5.3.2 Hybrid Role

When comparing themselves to the internal auditors, many interviewees emphasized the supportive aspects of their role and spoke about how important it is to know whom to talk to, or that it is very beneficial to have a coordinator who is responsible for each business function, since it can be challenging to talk with everyone.

*It is a lot easier to have a designated person to talk to, rather than always having to pull the jackets of the business managers. (Interviewee 4).*

*You do not want to build up too much administration with coordinators, people can talk to each other instead; but on the other hand, you run the risk of getting too involved I guess it would be different if we were bigger. (Interviewee 6)*

These in-between coordinators were mentioned as crucial to ensuring that a continuous monitoring and control process was followed. This was because they were able to be more involved with the specific function, while simultaneously functioning as the voice inside the business. The smaller firm was less inclined towards these coordinators and considered them unnecessary. However, time limitations and a lack of resources were mentioned as problems, and the larger firms often mentioned how the function of the coordinators was to mitigate these issues, since these coordinators would work full time with risk between the first and second lines. Kaplan & Mikes (2016) refer to the dual or hybrid role, where the organisation divided risk controllers into embedded and independent controllers with a view to resolving the tension between the independent challenge and advisory roles. It is submitted that beyond a certain size the tension is too large to ignore, and these coordinators become necessary.

5.6 Summary

The interview material yielded a substantial discussion on the nature of the operational risk controllers’ role in the financial sector. Several important challenges emerged, such as the challenge of conveying a message that enables the risk owners to recognise the benefits of an efficient risk management framework. In addressing this challenge, humility and confidence were mentioned as important, along with an ability to talk risk in a less complicated and more business-oriented manner. The other challenge was related to the long-term implementation and maintenance of processes and controls, since this can be challenging to achieve in practice.

In addition, it was established that the fundamental challenge was prioritization and to achieve long term change. Prioritisation was related to enabling the risk owners to make sense of and structure the information in a way that enabled the risk owners to make forward-looking and informed decisions that took the overall picture into account.

The analysis was based on three roles of the sensemaking risk controller, the independent facilitator, the engaged toolmaker, and the information interpreter. First, the analysis of the risk
controllers as an independent facilitator illustrated how risk controllers focus on facilitating discussion, and how relational and networking skills are much more important than technical capabilities. Second, the analysis of the risk controller as an engaged toolmaker revolved around how they worked to formalize the risk methodology throughout the organization. It became clear that the challenging aspect was not to get people to report, but rather to make them understand the value of reporting, and consequently get them to engage with the system more effectively. Finally, the analysis of the risk controller as a non-financial manager illustrated how multiple sources of data – both quantitative and qualitative – are used when framing discussions about risks in the organisation and how illustrating indirect financial impacts are in focus for many risk controllers, since there in general is less agreement about the relevance on this type of information and it remains a challenge for risk controllers to showcase its potential impact. Thus, risk controllers seek to quantify these impacts using multiple sources and methods and this role of managing and interpreting non-financial information is seemingly becoming more important by the day.
Operational risk management in financial services firms is about safe processes, robust controls, risk identification, and having routines to manage these various aspects (Chapelle, 2018). However, there are always people behind each part – they make sure that processes function and that routines are upheld. People make sure that things are managed, and our analysis suggests that the deciding factor for any risk controller is being able to reach out to the persons in charge of managing the risk and find a mutual understanding. A mutual understanding essentially means that the risk owners agree to the risk-based perspective provided by the risk controller. It is central for a risk culture that this understanding is reached and that the risk owners understand the value of activities such as incident reporting.

In line with this, the literature discusses how risk controllers become influential in different ways. Moreover, it recognizes that there is an increasing emphasis on the risk controllers’ ability to adopt a softer approach that focuses more on different ways of changing norms and behaviours within the organization (Mikes, 2016; Hall et al, 2015; Palermo, 2016, Fernando & Hall, 2016). The analysis provided in this paper lends support to the view that the role of risk controllers should be less about formal risk management tools and techniques, and more about the independent facilitation of a cross-functional language of business (cf. Mikes, 2016), the translation and reconfiguration of risk tools in a way that utilizes user input to create engagement (cf. Hall et al, 2015), consideration of how technology affects culture (cf. Palermo, 2016), the tension that exists between formalized processes and proactive discussions about risk (cf. Fernando and Hall, 2016), and the management of non-financial risk such as reputation (cf. Chapelle, 2018). In summary, this empirical analysis showcases how the most significant challenge in the role is to influence the risk behaviour in the business lines which is like (cf. Palermo, 2016, Mikes, 2016). However, we have expanded on the understanding on how risk controllers can work to successfully change the way organisations manage and perceive strategic uncertainties, our study has also shed light on the sensemaking perspective on risk management and its relevance in understanding the nature of the role of risk controllers in the financial sector.

To continue, our analysis has indicated how humility, too, is necessary in the first line communication, and why this is not viewed as something important, despite being a control function. A gloves-off approach was preferable, even though integrity and independence were considered crucial in being able to point out observable problems. A main finding of our research revolves around the role of risk controllers in transferring a risk-based perspective onto the risk owners. Transferring means combining different perspectives and finding a mutual interpretation of information that require a subjective interpretation. The transferring requires a way with people and an ability to understand multiple perspectives – one does not convince anyone without first understanding their concerns and priorities.
Moreover, a related finding was the importance of enabling the risk owners to understand a larger organizational context. Even if risks are managed in individual business functions that have the main responsibility, this does not mean that risk is only their concern. System failures, data protection, and other reputational issues concern the entire organization, and therefore part of the new role involved mapping out who the risk owners were rather than focusing on measuring risk. This is to some extent related to discussions about the problems with formalized procedures and how they displace meaningful discussion (cf. Hall & Fernando, 2016).

Furthermore, we found that while the risk controller gathers data in different ways, the most important data typically call for the risk controller to work in an embedded fashion with the business lines, since this enables the right questions to be asked. The role involves understanding whether a measurement is effective and captures what it is supposed to; it also involves understanding what is being monitored and what is not. All critical systems, products, and processes cannot always be monitored, and the work requires the risk controller to understand what to prioritize. The harsh reality is that prioritization is impossible without the knowledge of the risk owner. The role of the risk controller is to pose the right questions when gathering data: What system is the most critical? Which holds the most data? Which processes are being monitored and which not? Posing these questions is just as much about raising awareness among the risk owner as it is about ensuring that the right things are measured. According to the literature raising awareness and affecting norms and behaviour is essential (cf. Mikes, 2016, Palermo, 2016), however we posit that there is a need for research examining what it means to ask the right question in different context, are there barriers between business functions that can be addressed?

At the other end, the risk controller needs to create an environment that leads to long-term change, and a related challenge is ensuring that regulations and policies are continuously managed. Maintenance of routines, controls, and processes is vital, and relying on one-time overhauls can be an issue if a clear process for how to monitor something is not put in place. Even if a process is in place, it is not a given that the user will follow the process, since it needs to be performed by people who would much rather focus on their business enterprises. Risk management controls and processes are things that are added to the regular operation, and therefore the way people interact with risk tools and techniques is of the utmost importance (cf. Hall et al, 2015, Palermo, 2016, Jordan et al., 2013). Engaged toolmaking is a role in which risk controllers adapt risk techniques in cooperation with the user, to better adjust them to the business. The risk controller relies on this input to configure external tools or create new ones, which creates an engagement around the use of the tool that becomes a sustainable change to the way risks are managed. Understanding the benefits of continuous management and maintenance of routines, processes and controls is essential for any organisation and risk controllers needs to embrace the challenge of integrating external techniques using the knowledge that exist within the organisation, thereby ensuring a long-lasting change.

Culture is a deciding factor in relation to risk technology (cf. Palermo, 2016). Ensuring a vigorous incident reporting system where people understood the value and content of what should be reported is still a focus of many risk controllers. The way of formalizing the reporting is also important. Requirements or punishments for reporting such as a system where more
incidents automatically result in a critical and red rating could be detrimental to the risk culture, since this would lead to incidents not being reported. Qualitative trends were preferred in order to avoid the problem of measuring in a way that would punish people for reporting. Trends on how many of the incidents that had been solved enabled a positive culture of reporting in which technology and culture were considered. For risk controllers, regulators and senior management the lesson should be that more rules and regulation can have the opposite affect and that the risk culture needs to be protected by giving people some leeway and chance to influence the formalisation and e.g. give their input in systems concerned with incident reporting.

Finally, we found that data gathering is a large part of the role, and the risk controller has a responsibility to aggregate and report to senior management. Therefore, a risk controller might be tempted to formalize and codify the work of the risk owners excessively (cf. Hall & Fernando, 2016), but it is unfortunately often necessary to quantify if attention is needed. Financial impacts often speak for themselves, and this analysis suggests that risk controllers put a lot of time into and emphasis on achieving a kind of management of non-financial risks, such as IT disruptions, that do have an indirect financial impact – this against the background of criticism in the literature of attempts to quantify everything (cf. Power, 2009). These attempts to quantify non-financial risk hold a lot of promise in illustrating the value creation of effective operational risk management.
Getting organisations to implement a way of thinking about risk, where everyone – regardless of what business line they belong to – think from a risk perspective. This is the dream of many operational risk controllers, but far from a reality. Since the Lehman crash there has been a gradual shift towards making this happen. However, to achieve a change of this magnitude takes time; most people are not used to working in a risk-based manner, and to implement a corporate culture takes time and will not happen overnight.

The purpose of this research was to understand the nature of the role of operational risk controllers in the financial sector. What characteristics are important? How does the risk controller interact with other layers of the organization? How are tools used by the risk controller to drive change? This paper’s interpretation is that operational risk controllers have abandoned the approach where the focus is merely on the accuracy and quality of available information. Today’s risk controllers focus their attention on helping the decision-makers make sense of the business environment. They play an instrumental role when decisions are made, since their way of framing the organisational environment through tools, systems, relational interaction, and informal networks (Hall et al, 2015, Palermo, 2016. Mikes, 2016) forms the basis for the decision-makers’ views on risks and opportunities. Coming to this realisation, risk controllers also need to realise that their knowledge is limited by the fragmented and complex information that is a given in today’s digital era. Multiple sources of information are required even to get close to having a complete picture of all the vulnerabilities and exposures.

However, it is foolish to think that a complete picture can be achieved. Instead, the risk controllers should focus on independently facilitating the risk framework through a cross-functional risk language, (Mikes, 2016) and a softer approach with more focus on forming a mutual understanding with the risk owners. The risk controller should also focus on adapting tools to fit the business lines by gathering and integrating managerial input into the reconfiguration of tools, thus creating engagement around the implementation (Hall et al, 2015). Finally, the risk controller should focus on carrying the torch for non-financial risks that have an indirect financial impact, which are often ignored by the business. It will require innovative thinking in terms of finding new ways to quantify, for example, IT disruptions or reputational damage.

Three suggestions for further research are put forward. First, the present study only provides a snapshot of the nature of the risk controllers’ role in the financial sector. As indicated in the introduction, the second line has several important responsibilities, as operational risk management is simply called risk management in other industries. It would be interesting to study the role of these risk controllers over a prolonged period in a case study, for example. Such a prolonged format would result in even more detailed knowledge about how they play a potentially determining role in framing the environment for decision-making, or how they communicate with the business lines in the formatting of risk tools.
Second, the present study emphasises only the second line’s point of view, and there is a need to understand the situation from a first line perspective. How does the first line perceive the work of the second line? Do they feel involved and engaged in the toolmaking process? Do they regularly meet and interact with the second line to increase their understanding of aspects related to operational risks and risk management? Finally, there is a need for further investigation into how organisations and risk controllers work with reputational risks such as brand damage or business disruption risks. In the case of risk controllers, it would be of particular interest to observe their approach in the potentially fruitful area of managing and advising on non-financial risks.
References


Appendix

Interview guide

The purpose of the study is to study the risk controller's role in identifying, controlling and reporting within operational risk in the financial sector. We thereby seek to increase understanding of how operational risk management has developed and how the individual's role has changed with the development.

Background

1. Can you describe your educational background and previous experience of operational risk?
2. What is your position within the bank?

Definition and framework

1. How would you define risk?
2. Can you describe the bank's risk management framework in general terms?
   - What is the biggest challenge in the bank's framework?

Objective and operational risk

1. What is the objective of operational risk management?
2. What is your role in helping the bank achieve new goals and opportunities?

Identification, assessment and managing

1. How do you work with risk identification?
   - Tools? Workshops, Risk Register, Key Risks?
   - Frequent risks include frequent risks
2. How does the risk function map the organization to identify and analyze where operational risks can arise?
3. How do you work towards the risk owners?
   - Challenge versus oversight?
   - Sampling or trust in systems?

4. Is it hard not to get too involved with the first line?
   - How do you affect?
   - Learning new methods?
   - Involved other functions, know who to talk to?
   - Risk Language
   - Difference to IA?
**Monitoring and reporting**

1. Can you describe your responsibilities in risk reporting?
   - Systems used?
   - Hard to get people to report?
   - How do you affect?
   - Management of non-financial risks

2. Is it possible to achieve a good balance of too much and too little information in the reporting at different levels?
   - Escalation-criterions?
   - Adaptation to recipients?
   - The same view as the board?

3. Can you give examples of when the risk function opposed or challenged a strategic decision?
   - Result
   - Receipt

4. What are the challenges in proposing and putting a risk appetite?
   - Quality titles data
   - Is your eyesight always in line with the board?

**Challenges**

1. Where do you see the greatest challenges ahead?
2. What threats or opportunities do you see in digital development?
   - AI
   - Cybercrime
   - Automation and controls / management
   - Dissemination of misinformation
   - Data management and value creation

**Thank you for attending!**