Norwegian School of Economics
Bergen, spring 2016

Understanding Risk Appetite

What is it, what pressures shape it and how is it institutionalized

Håvard Baunan and Joel Berge

Supervisor: Anita Meidell

Master's thesis in Business Analysis and Performance Management
Economics and Business Administration

NORWEGIAN SCHOOL OF ECONOMICS

Abstract

The purpose of this thesis is to understand the concept of risk appetite in terms of what it is, what institutional pressures influence it, and how it is institutionalized in an organization. We try to understand what risk appetite is by examining the most influential enterprise risk management frameworks, reports from practitioners, and scholarly research on the topic. Through a case study of a large and complex Norwegian organization, we seek to explain what influences and institutionalizes risk appetite. First, we find that there is a consensus in the literature that risk appetite is a top-down element of enterprise risk management, but that there is disagreement as to how quantitatively it is understood and practiced. Second, we find that one cannot decouple risk appetite from its organizational context, as both external and internal institutional pressures influence risk appetite in the organization. Third, we find that risk appetite is not a singular concept in the organization. Risk appetites varies across risk categories, and the institutionalization of risk appetite relies on cultural elements in the organization. Our thesis adds to the understanding of the risk appetite concept, and adds to the scholarly argument that the evolution of risk appetite should go in the direction of addressing human and social behavior. Further, we contribute with a model to analyze institutionalization of risk appetite in organizations.

Acknowledgements

We want to thank everyone at Avinor that helped us with our research. We especially want to thank Ingvild Høydalsvik Røsæg at Avinor for being very helpful to us throughout the writing of this thesis. We would also like to thank the Centre for Applied Research at NHH (SNF) for allowing us to be a part of the Future-Oriented Corporate Solutions (FOCUS) program. We are very grateful for the scholarship we received from SNF that enabled us to travel for our research. We would also like to thank Katarina Kaarbøe for great input. Finally, we want to thank our supervisor Anita Meidell for supporting us through this thesis. You have been a great sparring partner, and we have received valuable tips and thoughtful comments throughout this semester.

Bergen, June 17, 2016

Håvard Hageberg Baunan Joel Berge

Table of Contents

List of figures

List of tables

“Not everything that can be counted counts, and not everything that counts can be counted”

- Albert Einstein

1 Introduction

1.1 Background and motivation

Several high profile environmental disasters, corporate scandals and the financial crisis of 2009 have increased the governmental push towards more control and better risk management (Woods, 2011). Coupled with the emerging belief that management systems are accountable (Spira & Page, 2003), the government response to such incidents has been to increase regulatory pressure on organizations to implement more effective corporate governance and internal control mechanisms (Soin & Collier, 2013). As a result, organizations have had to account for a broader base of risks (Spira & Page, 2003). This broader approach to managing risks, known as enterprise risk management (ERM), can be thought of as a more holistic approach to managing risk than traditional so-called "silo-based" risk management (Mikes, 2009). The Enterprise Risk Management – Integrated Framework (COSO, 2004) has adopted the concept of risk appetite as an important part of the ERM process, and defines risk appetite as "the amount of risk, on a broad level, an organization is willing to accept in the pursuit of value" (COSO, 2004, p. 19).

The COSO (2004) Enterprise Risk Management - Integrated Framework has come to be seen as the leading ERM framework (Power, 2009). As a thought leader, COSO (2004) suggests that risk appetite should govern many aspects of ERM and align the organization with respect to how much risk it is willing to assume.

Many have embraced the concept of risk appetite (Quail, 2012). However, risk appetite has also been a source of much discussion and debate among practitioners (ibid) and scholars (Power, 2009; Bromiley, McShane, Nair, & Rustambekov, 2015)

First, practitioners have embraced the concept of risk appetite (PwC, 2009; EY, 2015b; KPMG, 2008; McKinsey and Company, 2012; Deloitte, 2014). However, practitioners argue that risk appetite can be challenging to apply in organizations (KPMG, 2008; EY, 2015a) and that there are a variety of opinions about what it actually means to establish and embed risk appetite into risk practice (Deloitte, 2014).

Second, scholars have criticized ERM systems for being too mechanistic and to wrongfully rely on an "auditors logic" when assuming that risk can be handled in the same way as accounting figures (Power, 2009; Tekathen & Dechow, 2013; Paape & Speklé, 2012). Scholars argue that risk figures are very different from accounting figures, in that accounting figures are stable, while risk figures are not (Tekathen & Dechow, 2013). If ERM systems mimic financial reporting, then they promote an illusory, but cognitive comfortable world (Power, 2009). The concept of an overall risk appetite that can cascade through the organization is therefore the "epitome" of the intellectual failure of such ERM frameworks (ibid).

Bromiley et al. (2015) criticize the notion of risk appetite for being too vague, while Paape and Speklé (2012) argue that a formulation of risk appetite and risk tolerances does not contribute to "perceived risk management effectiveness" (p. 560). Bromiley et al. (2015) also question the core assumptions that "COSO-style ERM" is based on. Power (2009) argues, that in order to ameliorate these many shortcomings, the concept of risk appetite should be more concerned about human behavior and focus on risk appetite as a dynamic process involving a multitude of actors in an organization.

In the growing body of scholarly research on ERM, risk appetite has been given little attention despite the calls for further research (Van der Stede, 2011). Bromiley et al. (2015) argue that academic scholars have been slow to address the concept of risk appetite. It therefore seems to be a knowledge gap about risk appetite and how it is applied in an organizational setting.

Theoretically, we draw upon neo-institutional theory (Scott, 2014) to analyze risk appetite. We use Scott's (2014) understanding of institutions that states that "institutions comprise regulative, normative, and cultural-cognitive elements that, together with associated activities and resources, provide stability and meaning to social life" (Scott, 2014, p. 56). According to Scott's (2014) theoretical framework, there are three institutional "pillars" that intermingle and shape behavior in the organization (ibid). We argue that the analytical framework will provide a suitable theoretical foundation for analyzing how organizations understand and institutionalize their risk appetite.

In addition, we draw on Rosa's (1998) framework for understanding the concept of risk. This will give us a theoretical tool to help us analyze how risk categories differ in terms of how the

organization understands them. Moreover, we also draw upon Kaplan and Mikes' (2012) categorization of risk to help us structure parts of our analysis.

1.2 Research question

The motivation for this thesis is to add to our knowledge about risk appetite and explain how organizations understand their risk appetite. Thus, our main research question for this thesis is *how do organizations understand their risk appetite?*

We will answer this main research question by answering the following research questions.

i. *What is risk appetite?*
ii. *What institutional pressures influence risk appetite in an organization?*
iii. *How is risk appetite institutionalized in an organization?*

The first research question seeks to explore how risk appetite is understood in the enterprise risk management literature, among practitioners, and among academic scholars.

The second research question seeks to explain how institutional pressures influence the acceptable level of assumed risk in an organization. We do this by looking into how the organization's context influence its risk appetite by differentiating between internal and external pressures.

The third research question seeks to explain how organizations institutionalize their risk appetite, how ERM design and use may differ, and how risk perception and qualitative differences between risk categories may help explain the institutionalization

By answering these three research questions, we seek to understand how organizations understand their risk appetite.

1.3 Methodology

To answer our research questions, we use a qualitative research approach to analyze our empirical findings. To answer research question one, we draw on literature from enterprise risk management, practitioners, and academic scholars.

In order to answer our second and third research question, we conduct a case study of an organization that have introduced ERM and risk appetite in order to align the organization with respect to how much risk it is willing to take. In analyzing the collected data, we draw on neo-institutional theory (Scott, 2014) in order to answer the second research question. To answer the third research question, we use a combination of neo-institutional theory (Scott, 2014), risk perception theory (Rosa, 1998), and the risk categorization by Kaplan and Mikes (2012).

1.4 Relevance

First, we find that there is some disagreement about how quantifiable risk appetite should be as a measure for risk willingness in the organization. The risk frameworks and practitioners are positive of the concept, while many academic scholars are still to be convinced of its practical use in ERM. Second, we find that both external and internal institutional pressures influence risk appetite, and that risk appetite cannot be decoupled from its organizational context. Third, we find that there are several risk appetites, and that the institutionalization relies more on the organizational culture than formal rules and criteria.

This thesis is part of the growing body of literature on how to understand ERM systems in organizations. Our contribution adds to the knowledge of risk appetite by exploring the risk appetite concept in a broad sense. Furthermore, we contribute with an analytical model to analyze the institutionalization of risk appetite in an organization. Moreover, we try to answer the calls for further research on risk appetite by explaining how risk appetite is institutionalized through a case study.

1.5 Structure

The remainder of this thesis is structured as follows. In chapter two, we answer our first research question through a broad review of the risk appetite literature. In chapter three, we present the theoretical frameworks we use to discuss research question two and three. Chapter four contains our methodology and explains how we conducted the research for our thesis. We present our empirical findings in chapter five before we turn to our discussion in chapter six. In chapter seven, we conclude our research. Our references and appendix are found in chapters eight and nine respectively.

2 Risk appetite

Our first research question asks *what is risk appetite?* In this chapter, we will answer this question by exploring what has been said about risk appetite in the literature. We examine how risk management frameworks, practitioners, professional organizations, and academic scholars understand and define the concept of risk appetite.

2.1 Risk appetite in the risk management frameworks

Power (2009, p. 849) describes an ERM system as how "organizations should seek to identify all material risks to their objectives and sub-objectives, design controls and mitigations which produce a residual risk consistent with a target risk appetite, and monitor this entire process, making feedback adjustments as necessary". There are more than 80 ERM frameworks worldwide (Olson & Wu, 2008), and perhaps the most known framework is the COSO ERM framework (Hayne & Free, 2014; Power, 2009). However, while COSO have gained popularity in the U.S., other countries such as Canada, New Zealand, Australia, and the U.K. have adopted the international standard ISO 31000 (Woods, 2011). Additionally, we briefly look into how risk appetite is treated from a financial point of view in relation to financial regulations. In the following, we will examine how these three risk management frameworks discuss risk appetite.

2.1.1 COSO

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) was organized in 1985 with support from several professional accounting associations to support a private-sector initiative to combat fraudulent financial reporting (COSO, 2016). Over the last thirty years, COSO has published different frameworks where the Enterprise Risk Management – Integrated Framework (ERM-IF) is the most notable (COSO, 2016). The ERM-IF defines enterprise risk management as follows:

> Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its *risk appetite* [emphasis added], to provide reasonable assurance regarding the achievement of entity objectives (COSO, 2004, p. 16)

COSO (2004) introduces ERM as a continuous process for identifying opportunities and risks in pursuit of value, and argue that the process is an essential part of the organization's operational activities. Members of all organizational levels are part of the process to identify uncertainty (ibid). Their unique point of reference affects risk assessments and influences how organizations set objectives and put ERM mechanisms in place (COSO, 2004).

COSO (2004) defines risk as "the possibility that an event will occur and adversely affect the achievement of objectives" (p. 16). Furthermore, COSO (2004) defines risk appetite as:

> […] the amount of risk, on a broad level, an entity is willing to accept in pursuit of value. (p. 16)

The risk appetite is set in order to align the organization by setting risk tolerances, which are the amount of risk the organization is willing to accept for a given objective. COSO (2004) explains it as follows:

> In setting risk tolerance, management considers the relative importance of the related objective and aligns risk tolerances with risk appetite. Operating within risk tolerances helps ensure that the entity remains within its risk appetite and, in turn, that the entity will achieve its objectives (p. 16).

COSO (2004) argues that organizations need to adopt a "portfolio view" of risk. An organization often comprise of several units that might be subject to different risks, and a portfolio view enables top management to consider whether the overall risk portfolio is proportionate to the organization's risk appetite and potentially reevaluate "the nature and type of risks [the organization] wishes to take" (COSO, 2004, p. 60). For example, different risks may be within the different units' risk tolerances. However, taken together, the aggregate of these interrelated risks might exceed the organization's risk appetite (ibid). By adopting a portfolio view of risks, the organization can account for interrelated risks and make sure that the overall risk exposure is within its risk appetite (COSO, 2004).

COSO (2004) argues that management needs to possess a skillset of both quantitative and qualitative assessment techniques to assess its risk portfolio. Quantitative techniques rely on

the quality of the available data material and assumptions, while qualitative techniques rely on its effectiveness in capturing participants' "view on the potential likelihood and impact of future events, using either descriptive or numerical scales" (COSO, 2004, p. 53). Hence, the risk appetite can be articulated qualitatively, quantitatively, or both (ibid).

An organization's risk appetite must come before its strategy process, as it "helps management select a strategy that is consistent with [the organization's] risk appetite" (COSO, 2004, p. 28). Risk appetite should be reflected in the organization's strategy and objectives, which in turn guides resource allocation across the different units in the organization. Through strategy implementation, management keeps the organization aligned with its risk appetite (COSO, 2004).

After risk appetite and strategy are articulated, they are cascaded and operationalized through the organization using strategic objectives and risk tolerances (COSO, 2004), i.e. risk tolerances are risk appetite "applied" to specific objectives (Rittenberg & Martens, 2012). Risk tolerances are measured in the same metric as its related objective, and help the organization to stay within its overall risk appetite (COSO, 2004). Risk appetite and risk tolerances are important to the ERM system in terms of how to think actively and thoughtfully about the risks facing the organization, but also in guiding decision making and what risk level to accept in pursuit of the organization's different objectives (COSO, 2004; Rittenberg & Martens, 2012).

2.1.2 ISO 31000

The International Organization for Standardization (ISO) is a global non-governmental organization that develops and issues international standards (ISO, 2016), and released the risk framework ISO 31000 in 2009. However, ISO 31000 is a framework on how to implement risk management, and not a framework directly supporting the risk management process (IRM, 2010).

ISO 31000 emphasizes risk identification, risk analysis, risk evaluation, and risk treatment when implementing risk management, but does not include a risk appetite statement in the implementation process (ISO, 2009a). IRM (2010) notes that ISO 31000 is "silent" on the subject of risk appetite, and argues that this is surprising given risk appetite's role in other similar frameworks. However, the risk-vocabulary companion guide to ISO 31000 defines risk

appetite as “the amount and type of risk that an organization is willing to pursue or retain” (ISO, 2009b), but ISO (2009b) does not elaborate further on the concept.

2.1.3 Financial Stability Board

The Financial Stability Board (FSB) is an organization comprising many large industrialized nations’ central banks, international financial institutions, and standard-setting organizations (FSB, 2013). As part of its mission to promote financial stability and mitigate the issues concerning financial institutions that are “too big to fail,” the FSB released its “Principles for a Risk Appetite Framework” in 2013 (FSB, 2013).The report on risk appetite has been one of the standard-setting papers on the subject (PwC, 2014).

FSB (2013) defines risk appetite as “the aggregate level and types of risk a financial institution is willing to assume within its risk capacity to achieve its strategic objectives and business plan” (p. 3). Here, risk capacity refers to “the maximum level of risk the financial institution can assume given its current level of resources before breaching constraints determined by regulatory capital and liquidity needs […] as well as other customers and stakeholders” (FSB, 2013, p. 2). Risk appetite is the aggregate level of risk stemming from various risk categories, and the risk appetite statement should include quantitative measures of negative outcomes that can be aggregated and disaggregated, and qualitative measures that set the overall tone for the organization’s approach to risk taking (FSB, 2013).

FSB (2013) argues that risk appetite should be top-down leadership, but also that it should have bottom-up involvement from management at all levels. The organization and its management should check that the top-down risk appetite is consistent with the bottom-up perspective, securing a common understanding across the organization. This should be an ongoing and iterative process of evaluating the risk profile of the organization with the risk appetite (FSB, 2013).

The risk tolerances are the allocation of the organization’s aggregate risk appetite statement, i.e. the allocation of risk to the different levels in organization (ibid). These risk tolerances should be measurable in order to prevent organizations taking risks outside of their risk appetite (ibid). Because of issues arising from interrelated risks, FSB (2013) argues that the organization should uncover such interdependencies through stress testing of risks. Importantly, the risk

tolerances are the disaggregated elements of the quantitative risk appetite measurement. The qualitative risk measurements are not disaggregated in the same sense, but set the overall tone of the organization's approach to risk taking (ibid).

2.2 Professional organizations

There are a range of non-profit risk professional organizations and industry associations. We chose to examine the Institute of Risk Management (IRM) identified by Mikes (2011) as a professional body in the "global risk-management arena" (p. 230). As an example of one such organization, the IRM is a not-for-profit organization for professionals practicing risk management and publishes reports on risk management regularly (IRM, 2016).

2.2.1 The Institute of Risk Management

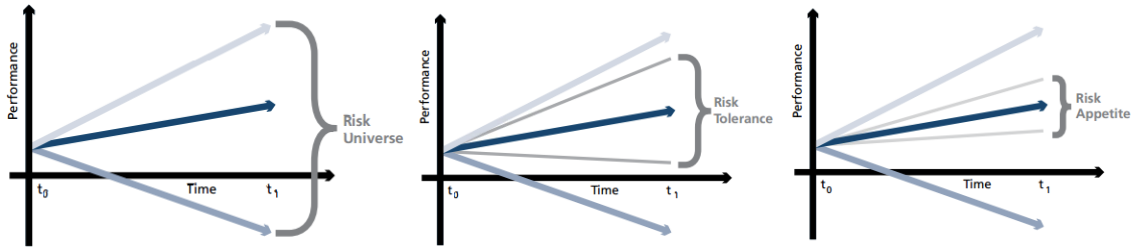
IRM (2011) argues that risk appetite is a "core consideration in any enterprise risk management approach" (p. 1). In their view, the goal is to "express clearly the extent of their willingness to take risk in order to meet their strategic objectives" (p. 1).

IRM (2011) argues that risk appetite is complex, and not a single, fixed concept in an organization. There may be a range of appetites for different risks, which need to align, and the appetites may vary over time as a response to changes in the organization's environment (IRM, 2011). The risk appetite needs to be measurable; if not, risk-appetite statements become "empty and vacuous" (IRM, 2011, p. 7). By measurable, IRM (2011) does not promote an "individual measurement approach" (p. 7) but argues that directors should understand how their performance drivers are impacted by risk.

IRM (2011) conceptualizes risk appetite and risk tolerance in relation to performance over time. The organization exposes itself to risks within a risk universe when moving in a direction. The risk universe represents all potential positive and negative outcomes. Within this universe, the organization expresses how much risk it can tolerate and set a measurable limit to that tolerance (ibid). Risk appetite is set within the risk tolerance to show how much risk the organization wants to take (IRM, 2011). In short, IRM (2011) explains that risk tolerances can be expressed in terms of absolutes, while risk appetite is about what the organization wants and how it goes about it (ibid). It is therefore the responsibility of the board to define both the risk tolerances

and the risk appetite in the ERM system (ibid). Figure 1 illustrates how these concepts relate to each other.

Figure 1 Risk appetite and risk tolerance



(IRM, 2011)

When it comes to the use of risk appetite, IRM (2011) argues that risk appetite "needs to be addressed throughout the organization for it to make any practical sense" (p. 8), i.e. the risk appetite needs to take into account differing views at a strategic, tactical, and operational level (ibid). The risk appetite must then be integrated with the culture of the organization (ibid).

2.3 Practitioners

Practitioners comprise the numerous audit and consulting firms, and other participants from the practicing risk management community. Financial organizations need to have specific risk appetite statements to be compliant with banking rules and regulations (KPMG, 2013) and with the recent push for better risk management and internal control in all organizations (Soin & Collier, 2013), practitioners issue reports and guidelines to help organizations with enterprise risk management and risk appetite.

2.3.1 Audit and advisory firms

The view of risk appetite as being the aggregate amount of risk that the organization is willing to accept, and that a risk appetite is set at the top level, is shared by many practitioners (EY, 2015a; EY, 2015b; KPMG, 2008; McKinsey and Company, 2012; Deloitte, 2014). We find several definitions of risk appetite are very similar to the definition of risk appetite expressed in COSO (2004) (KPMG, 2008; PwC, 2009).

There seems to be a focus on compliance among practitioners as risk appetite is part of the risk considerations and regulations that banks and financial institutions need to comply with (EY, 2015b; PwC, 2009). The risk appetite in financial organizations is not very flexible because of the regulatory environment that these organizations operate in (McKinsey and Company, 2012). However, risk appetite in "regular" organizations is a broader concept than in the financial sector. These organizations have a wider portfolio of risk that is not related to risk capital requirements (McKinsey and Company, 2012).

PwC (2014) argues that there is an agreement that the risk-appetite statement must include a balance between qualitative and quantitative components, what risk types the organization is exposed to and appropriate metrics that describe the risk appetite on an organizational level as well as a unit level (ibid).

A top-down approach is important to make sure that the risk appetite of the organization does not become a passive description of today's risk profile, but rather that it is proactive and forward thinking (PwC, 2009). To contribute to compliance and alignment across all levels, risk appetite is cascaded down in the organization to the risk categories that are relevant to the organization (EY, 2015a; PwC, 2009). However, to manage this process properly can be a managerial challenge (EY, 2015a; KPMG, 2008).

2.4 Academic scholars

To explore risk appetite from an academic point of view, we examined literature in the fields of management accounting, strategic management, and risk management.

2.4.1 Management accounting scholars

Meidell (2016) identifies thirty-three relevant peer-reviewed articles on ERM in high quality[1] management accounting journals. We searched each of the thirty-three articles electronically for the phrase "risk appetite". Twenty of the articles mentioned "risk appetite" at least once, and many of these papers did so while citing the definition of ERM given by COSO (2004).

[1] A high quality journal is defined by Meidell (2016) as a journal with a level four or level three ranking in the Academic Journal Guide issued by the Association of Business Schools (ABS).

Only three of the articles mentioned “risk appetite” more than ten times (Caldarelli, Fiondella, Maffei, & Zagaria, 2015; Paape & Speklé, 2012; Power, 2009). In the following, we will briefly present the main arguments on risk appetite from these three papers.

Caldarelli et al. (2015) examines credit risk management in banks, and the authors discuss risk appetite mostly in relation to financial regulatory frameworks like Basel III and how scholars have argued that “strategy and risk appetite must be aligned” (Caldarelli et al., 2015). However, the paper does not seem to be relevant in our further treatment of risk appetite.

Paape and Speklé (2012) argue that risk appetite is considered a key concept and precondition for “COSO-type” enterprise risk management, and that COSO (2004) promotes a clear preference for quantification when it comes to risk appetite at lower levels. Paape and Speklé (2012) continue to argue that this view on risk management is mechanistic, and problematize if “such a view is realtistic or practicable” (p. 550). They find that formulation of risk appetite and risk tolerances does not contribute to “perceived risk management effectiveness” and argue that this challenges the core assumptions that COSO (2004) are based on (Paape & Speklé, 2012, p. 560).

Power (2009) is perhaps the one who directs the most attention to risk appetite and what he argues are the failings of the concept. Power (2009) argues that risk appetite as applied in COSO (2004) “impoverishes” risk appetite as an organizational process (Power, 2009, p. 850). One of the main problems is the assumption that organizations can develop a “singular” organizational risk appetite, and Power (2009) argues that this assumption is tied to the neoliberal idea of organizations as “enterprising selves”. In addition, Power (2009) argues, that even though COSO (2004) defines risk appetite as possibly both qualitative and quantitative, “COSO-style ERM principles limit the concept of risk appetite within a capital measurement discourse” (p. 851). In order to ameliorate these many shortcomings, risk appetite as a concept must be more concerned about human behavior and focus on risk appetite as a dynamic process involving a multitude of actors (Power, 2009).

2.4.2 Strategic management

While exploring the concept of risk appetite, we found that scholars from the field of strategic management have also taken an interest in risk appetite and ERM. Bromiley et al. (2015) review

the literature on enterprise risk management and argue that academic scholars have “been slow to address many of the core practitioner concepts” (p. 268) and that risk appetite is one of these concepts (ibid). Bromiley et al. (2015) criticize the notion of risk appetite for being too “vague” and argues that many questions are being ignored about what risk appetite really is. Bromiley et al. (2015) also challenge the notion that organizations can have a consistent risk appetite, and continue to argue that whether organizations can achieve a consistent risk appetite or not has yet to be shown empirically. Bromiley et al. (2015) propose that scholars must turn their attention towards what risk appetite means, if organizations can have consistent risk appetites at lower levels, how lower-level risk appetites are aggregated, and how this all affect organizational behavior.

2.4.3 Risk scholars

While exploring the risk appetite concept in scholarly research, we came across risk scholars that had done research on the topic of risk appetite. Aven (2013) compares different definitions of risk appetite from several risk management frameworks, and argues that the risk appetite concept, if interpreted correctly, has “a role to play in risk management” (p. 462). The review contains several definitions of risk appetite from different risk management frameworks, audit and consultancy firms, and government agencies. The definitions vary in what they choose to include in the risk appetite definition. Some definitions only comprise an appetite for loss or expected loss, while others also include a value dimension. An example of a definition that only includes the downside was “the level of risk that an organization is willing to accept” (p.464), while the definition “the amount of risk an entity is willing to accept in pursuit of value” (p. 464) also included a value dimension. Aven (2013) argues that a risk appetite statement that incorporates a value dimension may improve the risk considerations by shifting the focus from “isolated risk acceptability judgments” to more “balanced considerations” that are more in line with “basic principles of risk management” (Aven, 2013, p. 463). Aven (2013) proposes a general definition of risk appetite as “appetite for risky activities in pursuit of values” (p. 465).

2.5 Discussion

Many different voices discuss risk appetite in terms of what it is, how it is measured, set, and how it should be used. The following discussion is concerned with what the different voices say about the concept, its quantifiability, if it is top down, and its use.

First, the risk appetite concept is defined fairly similarly across the different frameworks (COSO, 2004; FSB, 2013; ISO, 2009b). However, the ISO 31 000 (2009a) framework does not mention risk appetite. We would have expected a more substantial treatment of risk appetite considering the extensive emphasis in COSO (2004).

We find that the audit and advisory firms also have the same understanding of the risk appetite concept (Deloitte, 2014; KPMG, 2008; PwC, 2009; EY, 2015b; McKinsey and Company, 2012). However, IRM (2011) proposes a very different understanding of risk appetite. As opposed to the singular and stable concept of the normative frameworks, IRM (2011) argues that there are multiple appetites for risk and that they are not stable. Moreover, IRM (2011) also defines risk tolerances in a different way. In this view, risk tolerances are not a disaggregation of the risk appetite but the upper limits to how much risk the organization can bear (ibid).

We find that the scholarly research use, for the most part, the COSO-definition when they criticize risk appetite (Paape & Speklé, 2012; Power, 2009; Spira & Page, 2003; Bromiley et al., 2015), and some scholars identify risk appetite as a precondition for "COSO-style" enterprise risk management (Paape & Speklé, 2012). However, Aven (2013) found that while the definition of risk appetite were many, they essentially said the same just with or without a value component (ibid).

Second, many argue that risk appetite can be both qualitative and quantitative (COSO, 2004; Deloitte, 2014; EY, 2015b; PwC, 2009). The FSB (2013) also suggests that the risk appetite can be both, but that the quantifiable element should be applied through risk tolerances and that the qualitative element should "set the tone" for risk management in the organization. IRM (2011) argues that risk appetite need to be somewhat measurable in order to be useful. Power (2009), on the other hand, argues that risk tolerances effectively limit the risk appetite concept to a quantitative concept in the ERM context. Risk appetite is by many thought of as both a qualitative and quantitative measurement, however, the ERM frameworks' design lean towards a preference for quantitative measurements (Paape & Speklé, 2012).

Third, we find that there is a broad agreement that the risk appetite is a top-down element of the ERM system (COSO, 2004; FSB, 2013; IRM, 2011; Deloitte, 2014; EY, 2015b; KPMG,

2008; PwC, 2009), as it is the responsibility of top management and the board to define and articulate the risk appetite and its criteria. Power (2009) criticizes top down notion of risk appetite as he argues that risk appetite is more than a singular concept and that it should be more concerned with organizational processes (ibid).

Forth, COSO (2004) states that a risk appetite ensures risk alignment in the organization. The risk appetite should be set at a strategic level and then cascaded down in the hierarchy through risk tolerances to organizational objectives (ibid). FSB (2011) shares this view, as the quantifiable element of risk appetite is disaggregated to lower levels in the organization, while the qualitative element of risk appetite sets the tone of risk management (ibid). However, IRM (2011) take a more integrated approach, and argues that risk appetite should account for differing views about risk at various levels in the organization.

To summarize, risk appetite is considered a key building block that ERM systems rest on (COSO, 2004), but that there are differences in terms of what the risk appetite is, how to measure it, and how to use it. The common denominator is that risk appetite is the top-down element of ERM systems that should align the organization with respect to how much risk to assume. Table 1 summarizes what the different voices say about risk appetite.

Table 1 Risk appetite overview

	Risk appetite concept	**Quantifiable vs qualitative**	**Top down vs bottom up**	**Use**
COSO	Amount of risk on a broad level	Both quantifiable and qualitative	Top down element that guides the bottom-up feedback	Align the organization through setting risk tolerances to objectives
FSB	The aggregate level of risk	Both, but the qualitative element "sets the tone" for the organization's approach to risk taking	Top-down element that guides the bottom-up feedback	Alignment through disaggregating the risk appetite into tolerances
ISO	Amount of risk the organization is willing to pursue[2]			

[2] ISO 31 000 does not mention risk appetite, so the quote is in the words of its vocabulary guide (ISO, 2009b)

	Risk appetite concept	**Quantifiable vs qualitative**	**Top down vs bottom up**	**Use**
IRM	Not singular, but there are several appetites for different risks	Measurable in the sense that directors can understand how their performance drivers are impacted by risk	Top-down as it is the responsibility of top management to define both risk appetite and tolerances	Express the extent of their risk willingness with multiple risk appetites for risks that should be measurable
Audit and advisory practitioners	Amount or aggregate level of risks	Quantitative but increasingly qualitative depending on the risk exposure	Top- down element that guides the bottom-up feedback	Alignment through the cascading of risk appetite to risk categories that are relevant
Scholarly criticism				
Management accounting (Power, 2009) (Paape & Speklé, 2012)	Criticizes the notion of a singular risk appetite	Criticizes the clear preference for quantification	Criticizes the whole ERM concept as too mechanistic Questions the core assumption that COSO-type ERM are built on	Questions if risk appetite is realistic or practicable
Strategic management (Bromiley et al. 2015)	The concept is vaguely understood, and academic scholars have been slow to address the concept		Question how lower-level risk appetites are aggregated	Challenge the notion that organizations can have a consistent risk appetite Question the effect on organizational behavior
Risk scholars (Aven, 2013)	Argues that the risk appetite has a role to play in risk management			

3 Theoretical frameworks

In this chapter, we present the theoretical frameworks that we will use in our analysis of research questions two and three. To answer research question two, we will use neo-institutional theory (Scott, 2014) to analyze how institutional pressures (DiMaggio & Powell, 1983) influence risk appetite. To answer research question three, we will in addition to using Scott's (2014) framework, also draw on risk perception theory (Rosa, 1998) and the risk categorization suggested by Kaplan and Mikes (2012).

3.1 Neo-institutional theory

Institutional theory is the most dominant approach to understanding organizations (Greenwood, Oliver, Suddaby, & Sahlin-Andersson, 2008). Traditionally, scholars in organizational theory viewed organizations as "agentic" actors responding to "situational circumstances" by interpreting their contexts and taking actions. Together with other views like resource dependence theory, structural-contingency theory and behavioral theory of the firm, all these views tried to understand how organizations rationally adapted or reacted to a more or less fixed context or environment (ibid). The assumptions on which the organizational context were founded came from more of an economist tradition, and context was treated mostly as a market or "technical setting" (Greenwood et al., 2008).

Seminal papers in what is now called *neo*-institutionalism (or new institutionalism) were written in the late 1970s and early 1980s (Greenwood et al., 2008). These papers promoted the idea that organizations are *influenced* by their institutional context. According to Scott (2014), the focus on the cultural elements differentiates neo-institutionalism as it focuses on "shared conceptions of what constitute the nature of social reality [that] can create the frames through which meaning is made" (Scott, 2014, p. 67). This marked a shift away from the traditional view outlined above about how scholars viewed organizations (Greenwood et al, 2008). Over the next decades, a wide range of perspectives were explored and ambiguities emerged in the field, but "Scott (1995) brought order to the various strands of institutional analysis by distinguishing between the regulative, normative and cultural-cognitive […] elements that underpin institutions" (Greenwood et al., 2008, p. 15).

We draw upon Scott (2014) and his analytical framework in order to explain both how risk appetite is shaped by institutional pressures and how it is institutionalized. Scott's pillars has become one of the "most-cited contributions in the institutional literature" (Greenwood et al., 2008, p. 15) as he attempts to establish a relatively broad definition of institutions by gathering a number of ideas that have been proposed by scholars in the field of institutional theory (ibid). Scott's contribution was to sort these into the regulatory, normative, and cultural cognitive systems, also referred to as the three pillars of institutions (Scott, 2014).

3.1.1 Analytical framework: institutional pillars

Scott (2014) defines institutions as comprising "regulative, normative, and cultural-cognitive elements that, together with associated activities and resources, provide stability and meaning to social life" (p. 56). Important aspects of institutions and organizations are people and behavior. Institutions have an ability to both control and restrict human behavior through, for example legal and moral boundaries, and "institutions provide stimulus, guidelines, and resources for acting as well as prohibitions and constraints on action" (Scott, 2014, p. 58). In other words, the institutional pillars are building blocks of institutional structures, which guide behavior and resist change (ibid).

Previous scholars in the field of institutional theory have often chosen to place their emphasis on only one of the three different "pillars" of institutions and highlighting one as the most important ingredient of institutions. However, Scott (2014) choses to include all three pillars and focuses on identifying the similarities and differences between them, and argue that more than one pillar may be at play simultaneously. In general, the pillars form a continuum ranging from the conscious to the unconscious, from the legally enforced to the taken for granted (Hoffman, 2001).

These institutional effects can be observed both within and outside of the organization (Palthe, 2014). Even though Scott (2014) has identified six levels of analysis, we only distinguish between institutional pressures that stem from within the organization from those outside the organization, as suggested by Klovienė (2012). Distinguishing an internal institutional factor from an external depends on whether the institutional factor "performs" irrespective of an organization, or if it depends on the reaction of the organization (ibid).

The regulative pillar places emphasis on formal rules, monitoring and "explicit regulatory processes" (Scott, 2014, p. 59). Regulatory processes "involve the capacity to establish rules, inspect others' conformity to them, and, as necessary, manipulate sanctions – rewards or punishments – in an attempt to influence future behavior" (Scott, 2014, p. 59). Regulatory systems constrain behavior through the formalization of rule systems, which specify required conduct in an unambiguous fashion (ibid). Moreover, there is an instrumental rationale behind the regulatory pillar (Scott, 2014). Organizations craft laws and rules that they believe will advance their interests, and the individuals of the organization conform in order to avoid sanctions or seek rewards (ibid).

The regulatory pillar is less salient if laws or rules are "sufficiently controversial or ambiguous that they do not provide a clear prescription for conduct" (Scott, 2014, p. 62). Ambiguities are interpreted by organizational actors and rely on other institutional elements, such as culture or norms, rather than regulatory elements to have behavioral effects (ibid).

The normative pillar comprise normative systems that can constrain social behavior, but also empower and enable social action (Scott, 2014). For the normative pillar, both values and norms play an important role in determining appropriate behavior in an organization (ibid). Values are conceptions of a preferred or desired outcome with standards to assess behavior, whilst norms specify how things ought to be done, i.e. define legitimate means to pursue valued ends (ibid).

Normative systems define and set different goals for the organization, but normative systems also define the means by which the specific end or goal can be reached. Normative systems give rise to *roles*, as not all values and norms "are applicable to all members of the collective" (Scott, 2014, p. 64). Normative systems emphasize the logic of appropriateness, which implies that organizational actors evaluate the appropriate behavior given his or her role and the situation (ibid).

Cultural frameworks and symbolic processes are important as they work to "define the nature and properties of social actors and social actions" (Scott, 2014, p. 68). However, not everyone in an organization holds the exact same beliefs, and the degree to which cultural elements are embodied in, for example routines, will have an impact on how institutionalized cultural elements become (Scott, 2014). Yet, the most important element in the cultural-cognitive pillar

is the "role played by the socially mediated construction of a common framework of meanings" (Scott, 2014, p. 70). In other words, the shared understanding that is constructed through interactions between actors in the organization creates compliance through that shared understanding (ibid).

3.1.2 Institutional pressures

DiMaggio and Powell (1983) identify three forms of institutional pressures that shape organizational behavior –coercive, normative, and mimetic. These are pressures towards isomorphism, i.e. pressures toward accommodation with the outside world (ibid). This concept of institutional isomorphism is included in Scott's (2014) institutional pillars, and is a useful tool for understanding modern organizational life (DiMaggio & Powell, 1983). In light of Scott (2014), these pressures are thought of as mechanisms of control of organizational behavior and that these are distinctive for each respective institutional pillar, i.e. coercion is attributed to the regulative pillar, normative is attributed to the normative pillar, and the mimetic pressures are attributed to the cognitive-cultural pillar (ibid).

Coercive pressures stem from both formal and informal pressures exerted on organizations by other organizations by which they are dependent (DiMaggio & Powell, 1983). Coercive pressures can be "felt" as a force to respond to a political decision or mandate, e.g. conformity with governmental standards (ibid). Coercive pressures can also occur outside the governmental arena, for example in a group where subsidiaries need to be compliant with the policies of the parent corporation (ibid). In light of the institutional pillars, rules and laws indicate such pressures, and the basis of compliance for such coercive pressures is expedience, i.e. to say that compliance happens in order to avoid sanctions (Scott, 2014).

Normative pressures come from what DiMaggio and Powell (1983) call professionalization. Professionalization is defined as "the collective struggle of members of an occupation to define the conditions and methods of their work […]" (p. 152). Formal education and professional training can create normative pressures as they promote normative rules about organizational and professional behavior (ibid). In light of Scott (2014), normative mechanisms can be coupled with a social obligation to comply with such normative rules. Furthermore, indicators of the normative pillar can be certification or recognition from the professional community (ibid).

Mimetic pressures are primarily a result of uncertainty (DiMaggio & Powell, 1983). That is, when an organization faces a problem with ambiguous causes and unclear solutions, a problemistic search is set in place (ibid) and develops a shared understanding or a set of collective meanings that condition how organizational actors interpret and respond to the world around them (Scott, 2014). The basis of compliance for mimetic pressures is therefore a shared understanding or a "taken-for-grantedness" (ibid). Furthermore, the prevalence of a set of common beliefs or shared logics of action are indicators of mimetic pressures in the organization (ibid).

The combination of the institutional pillars (Scott, 2014) and institutional pressures can summarized in the following table. The table is a slightly modified version of Scott's (2014) table for the three pillars of the institution.

Table 2 Institutional pillars and pressures

	Regulative	**Normative**	**Cultural-cognitive**
Pressures	Coercive	Normative	Mimetic
Basis of compliance	Expedience	Social obligation	Taken-for-grantedness Shared understanding
Indicators	Rules Laws	Certification Recognition	Common beliefs Shared logics of action

3.1.3 Institutionalization

Institutionalization is a process that happens to an organization over time (Selznick, 1957) and is the emergence of "orderly, stable, social intergrading patterns out of unstable, loosely organized, or narrowly technical activities" (Selznick, 1992, p. 232). The rationale is that institutionalization is "the social creation of reality" (Berger & Luckmann, 1967, p. 15). The first step in institutionalization is the creation of formal structure that provide an "institutional" solution to problems of coordination (Scott, 2014), e.g. explicit goals and rules in the organization (Selznick, 1992). The second step is the process of making the institutional solution a part of the social reality (Scott, 2014). "Thick" institutionalization is a term used for organizational solutions that have a broad institutionalization in the organization, i.e. the pillars support and reinforce one another (Selznick, 1992).

In answering questions such as how institutionalization occur, Scott (2014) states that the typology of DiMaggio and Powell (1983) is useful as it "focuses attention on three contrasting mechanisms – coercive, normative and mimetic – that identify various forces or motives for adopting new structures and behaviors" (Scott, 2014, p. 158). As previously mentioned, these forces or motives for adopting new behavior are arrayed in line with the three pillars of the institution.

3.2 Risk perception

Risk has always has been a part of the human endeavor, but it has a short history in academic literature (Rosa, 1998). The definition of risk has evolved in "divergent approaches and traditions that show no sign of rapprochement" (Hansson, 2010, p. 231). These divergent approaches are represented by two competing paradigms; the positivist paradigm that views risk as an "objective" concept, and the constructivist paradigm that views risk as a subjective social construct (ibid).

On the one hand, the positivistic paradigm is the dominant view in technical literature and applied sciences, and is often referred to as "objective" risk (Hansson, 2010). This paradigm distinguishes sharply between perceived considerations about risk and "objective" facts about the outcomes and their probabilities (ibid). Some scholars propose to subtract immeasurable aspects out of the risk definition, and term it "uncertainty" (Knight, 1921). This narrow definition is widely adopted by technical analysts as it allows for comparison of dissimilar hazards by converting the "objective" fact in to one common metric (Rosa, 1998). However, a pure positivistic understanding of risk can cause a realism-objectivism bias, which is the result of reducing and ignoring values such as "social, political, and cultural context that shape risk considerations" (Rosa, 1998, p. 21).

On the other hand, the constructivist paradigm has its conceptual roots from sociology, especially the cultural theory of Douglas and Wildavsky (1982). In general, cultural theory tries to explain how people perceive and act upon the world around them (Oltedal, Moen, Klempe, & Rundmo, 2004). The reason why the theory has had a powerful voice in the discussion of risk perception is arguably that risk is impossible to sense as it refers to something "out there" (Oltedal et al., 2004). As a result, risk is all about subjective thoughts, beliefs, and constructs

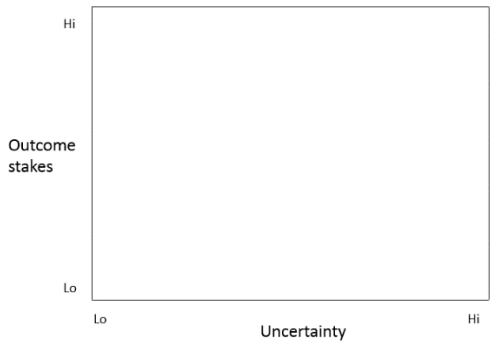
(ibid). The cultural theory understands risk as a cultural phenomenon and as a representation of our collective belief system (Rosa, 1998). The constructivist paradigm sees the world as a product of our actions of continuously negotiating the meaning of the world (ibid). If taken to the outer limits, the constructivists see reality as entirely subjective and that our "negotiated knowledge of the world is the functional equivalent of the world itself" (Rosa, 1998, p. 21). As a result, our perception of risk is the functional equivalent to risk itself (ibid).

In contrast to the realism-objectivism bias of the positivistic paradigm, the constructivist paradigm presents a constructivist bias by omitting realism from the definition (ibid). This notion is problematic since some risks are real regardless of how an individual perceives it, e.g. the risk of death (ibid). Furthermore, if risk has to first be perceived to actually exist, then any danger an individual is unaware of would fall into the category of ignorance, which in turn is a form of risk in itself, thus leaving out any form of realism could cause a biased understanding of risk (ibid).

Each of the two paradigms pose two extreme positions with opposite foundations, with their strength and weaknesses (ibid). Rosa (1998) argues that both of them are poor descriptions of reality, and that a more sensible approach is to combine the two paradigms in a continuum as there is no clear line between the two paradigms (ibid).

In the integrated approach, risk is defined as "a situation or event where something of human value (including humans themselves) has been put at stake and where the outcome is uncertain" (Rosa, 1998, p. 28). The definition includes three elements. First, the notion that risk expresses some state of reality of human concern or interest. Second, the distribution of possible outcomes goes both ways i.e. both positive and negative outcomes. Third, the idea of uncertainty, in the sense that humans do not know if an outcome will or will not occur (ibid). From this definition, Rosa (1998) introduces two dimensions to risk that make up the axial continuums of Figure 2.

Figure 2 The dimensions of risk



(Rosa, 1998)

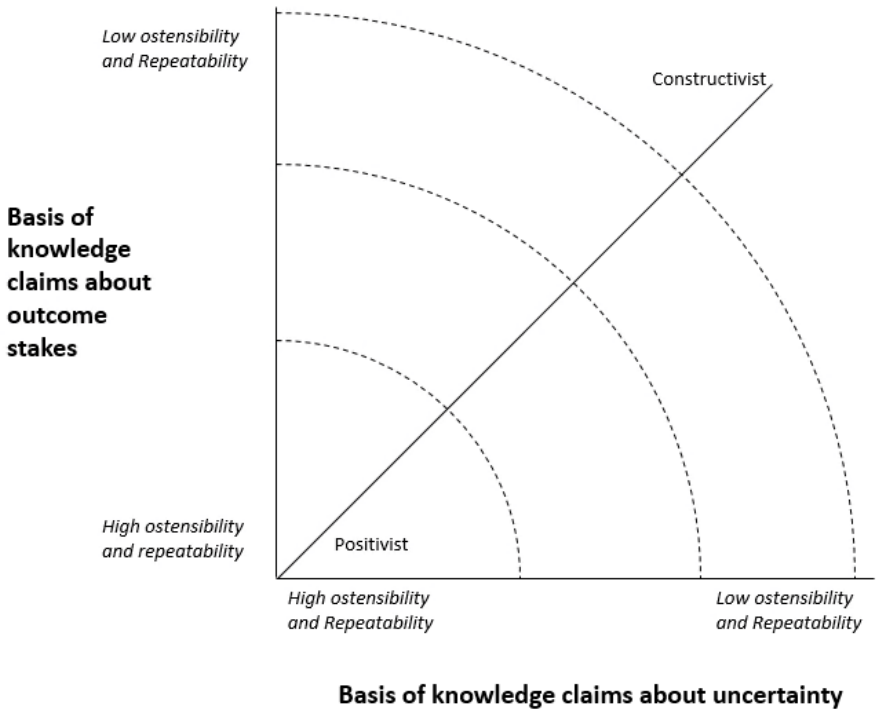
Rosa (1998) suggests that the knowledge claims about these dimensions may vary in terms of the evidentiary basis of claims to knowledge, i.e. not all claims about risk have the same availability of objective facts. There are two guiding principles that provide a way of deciding the placement of knowledge claims along the continuum of epistemic agreement (ibid), i.e. if there is an inter-subjective agreement about the knowledge claim. Moreover, the two guiding principles place risk claims along the continuum whereas knowledge claims are highly relativistic (truth is relative) on the one end, and highly realistic (truth is objective) on the other end (ibid). The two principles are *ostensibility* (I can point to examples) and *repeatability* (the examples will repeat themselves) of the knowledge claim (ibid).

The ostensibility principle asks whether "you see what I see", and if the answer is "yes" then there is inter-subjective agreement (ibid). The greater the agreement, the higher placement in the hierarchy. If the knowledge claim does not produce inter-subjective agreement then the repeatability criterion responds, "just wait and you will have another opportunity to observe what I see" (Rosa, 1998, p. 35). On the one hand, if the ostensibility criterion is met, then the repeatability criterion is also likely to be met. On the other hand, if a knowledge claim should fail these criteria, then the realism logic fails, and we need to look toward constructivism and related perspectives as a way of understanding it (ibid).

In this integrated view, no knowledge claim can be absolute. Rather, human perception can only approximate the world we seek to explain (ibid). In a pragmatic sense, it denies that all knowledge claims are equal, but that the quality of claims depend on the level of agreement it

evokes (ibid). This is illustrated in Figure 3, which is a modified version of Rosa (1998) realism-constructivism continuum of knowledge clams about risk.

Figure 3 Realism-constructivism continuum of risk



(Rosa, 1998)

3.3 Risk management framework

Kaplan and Mikes (2012) suggested a framework for ERM that differentiates between risks based on the "qualitative distinctions among the types of risks that organizations face" (ibid). The authors identify three distinctive categories: preventable risks, strategic risks, and external risks (ibid).

Preventable risks are risks that arise from within the organization that do not offer any strategic benefit to the organization (ibid), i.e. risks that offer no upside. These risks are controllable and ought to be eliminated or avoided as far as it is sensible from a cost-benefit perspective (ibid).

Strategic risks are risks that offer strategic returns, i.e. both an upside and a downside (ibid). The difference between preventable and strategic risk is that the strategic risk is not inherently undesirable (ibid).

External risks are risks that arise from events outside the control of an organization and is outside their area of influence (ibid). Such risks could be "political disasters or major macroeconomic changes" that affect the organization (ibid).

3.4 Assumptions

The second research question is *what institutional pressures influence risk appetite in an organization?* We assume that pressures that stem from both within and outside the organization, influence risk appetite. Furthermore, we assume that risk appetite is not decoupled from its organizational context as coercive, normative, and mimetic pressures shape what level of assumed risk the organization deems acceptable.

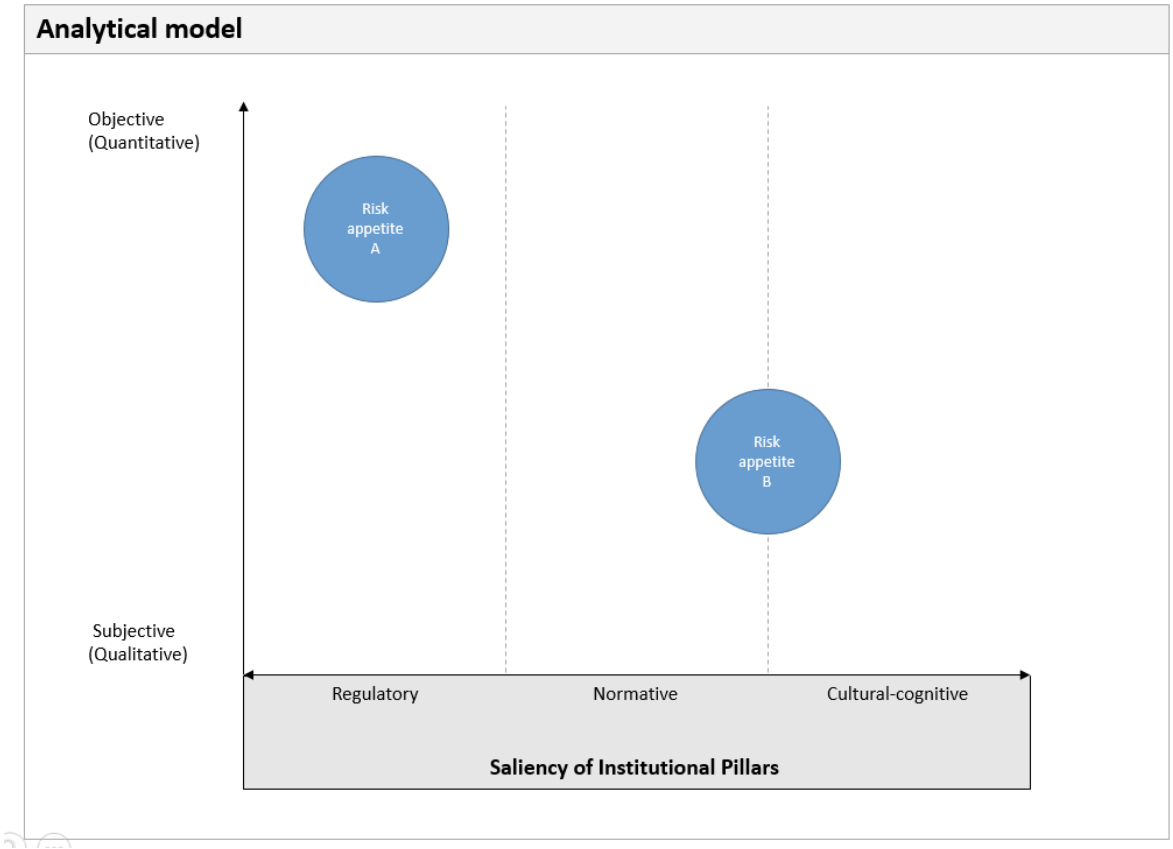
The third research question is *how is risk appetite institutionalized in an organization*? By combining the theory of institutional pillars (Scott, 2014) and Rosa's (1998) model of risk perception, we made an analytical model for analyzing the institutionalization of risk appetite in an organization.

In the analytical model, the focus is on the saliency of pillars, meaning that we do not devote much attention to the "thickness" of the institutionalization of risk appetite. Rather, our attention is on which of the regulative, normative and cultural-cognitive pillars that are most important in determining what level of assumed risk is considered acceptable for the different risk categories. We identify the saliency by analyzing which of the coercive, normative, and mimetic mechanism that shape the acceptable level of risk. We acknowledge that multiple pillars can support and determine acceptable behavior simultaneously, yet the focus of the analytical model is the saliency of the pillars as an organizational actor rationalizes what is acceptable organizational behavior.

We present the analytical model with two examples in Figure 4. The first axial continuum is concerned with how subjective or objective a risk category is. The first axis is a simplification

of Rosa's (1998) model where we use the more common terms objective (quantitative) and subjective (qualitative). The second axial continuum is concerned with the saliency of the institutional pillars. The rationale is that even though many pillars shape organizational behavior, not all are equally salient.

Figure 4 Analytical model



The analytical model help to structure and visualize our analysis of the institutionalization of risk appetite in an organization. To illustrate, here risk appetite A is more quantifiable, and therefore more objective. Organizational behavior is shaped by means of coercion, which is indicative of the regulatory pillar. Risk appetite B is not as quantifiable as A, and thus not as objective. B relies on more normative and mimetic mechanisms for its behavioral effects, which are indicative for the normative and culture-cognitive pillars.

4 Research methodology

The purpose of this chapter is to elaborate how we answered our main research question *how do organizations understand their risk appetite?* We will first state our research philosophy, as it influences our research design and data collection (Saunders, Lewis, & Thornhill, 2009). Second, we explain our research design, i.e. the purpose and strategy. Third, we explain how we collected the primary data and secondary data, respectively. Forth, we explain our research approach and the process of analyzing the collected data. Fifth, we evaluate our methodology through Lukka and Modell's (2010) authenticity and plausibility aspects and briefly describe how we handled some ethical issues, as suggested by Yin (2003).

4.1 Research philosophy

We find that it is important to briefly explain and discuss our philosophical underpinnings, since philosophical commitments influence both what choices we make and how we understand what we are investigating (Saunders et al., 2009).

We are pragmatic in the way we answer the research question. Lukka and Modell (2010) argue that a pragmatic research philosophy acknowledges both that there can be several truths and the role of consensus of views in social settings. However, Lukka and Modell (2010) deny the notion that all truth claims are equally justifiable. In other words, it integrates social constructionism and a modern form of realism (ibid). This implies that there is no truth as a singularity, but there is a zone within which our truth claims have to fall in order to be viewed as valid in social settings (ibid). This philosophical viewpoint is also consistent with our chosen theoretical framework for understanding the risk concept, as it requires an "epistemological hierarchicalism", i.e. it denies that all knowledge claims are equally fallible (ibid).

The practical implication of the pragmatic philosophy is that the focus is not on methods per se, but on the research question and how to answer it (Creswell, 2007). As a result, the researchers have freedom to choose the methods, techniques, and procedures that best meet their needs and purposes (ibid).

Answering our main research question: *how do organizations understand their risk appetite,* we use the methods, theories and procedures we find most helpful in providing us with an

answer to the overarching research question. In the following sections, we explain what we chose to do and discuss why this helped us answering our research question.

4.2 Research design

The research design is, in a broad sense, a general plan for how to answer the research question (Saunders et al., 2009). The research design provides the reader with the logic that links the collected data and the conclusions drawn, to the initial research questions of the study (Yin, 2003).

4.2.1 Purpose of the research

It is common to classify research purposes as either exploratory, descriptive or explanatory (Saunders et al., 2009). However, just as a research question can be both descriptive and explanatory, a research project can have multiple purposes (ibid). First, the exploratory study is conducted when there is uncertainty around the nature of the problem and one wishes to clarify the understanding of the problem. This is particularly useful when the researcher wants to find out what is going on, to seek new insight, or shed new light over a phenomenon (Robson 2002, as cited in Saunders et al., 2009). Second, a descriptive study is conducted when the researcher have a clear picture of the phenomenon of interest. In contrast to the former approach, the researcher tries to make a precise or accurate picture of persons, events or situations. Third, an explanatory study typically seeks to explain causal relationships between variables (ibid).

The purpose of this thesis is to explain how organizations understand and institutionalize risk appetite. As such, the purpose of this thesis is explanatory. However, generating explanations does not mean that we, as researchers, have to subscribe to an ontology characterized by "naïve realism" (Lukka & Modell, 2010). Rather, it means that there is:

> No reason whatsoever to detach the emic understandings of situated meanings of people from explanations, but rather vice versa: those meanings can be seen as including their causal implications, and without understanding them it can often be impossible to explain, or ''make sense of", what is going on in the social world (Lukka & Modell, 2010, p. 466).

We provide explanations based on the careful analyses of risk appetite in a real-world organization with all its complexities. This is a suitable position to trace causal linkages between the examined phenomena (Lukka and Modell, 2010). The rationale is that interpretive research can produce explanations from a more external viewpoint because dependencies developed from profound emic understandings tend to be more than merely subjective mental states (ibid). An emic understanding is to say that we provide the perspectives and words of the research participants, and not our interpretations of it.

In other words, we seek to explain dependencies in how an organization understands and institutionalizes risk appetite through the development of thick explanations, i.e. explanations based on emic understandings (Lukka & Modell, 2010).

4.2.2 Research strategy

Saunders et al. (2009) propose seven different research strategies for business research. However, instead of outlining all the strategies, we thoroughly explain the rationale behind why we chose the case study strategy in answering our research question.

We argue that the case study is an appropriate research strategy for the following reasons. First, according to Saunders et al. (2009), the research question should guide the choice of strategy in a way that is coherent with the amount of time, philosophical underpinnings, and resources. As our research question has an explanatory purpose as we seek the answer *how do organizations understand their risk appetite?* We answer this by looking at *what institutional pressures influence risk appetite,* and *how risk appetite is institutionalized in an organization.* The case study strategy is well suited to generate answers to questions, such as why, what, and how (Saunders et al., 2009).

Second, Yin (2014) defines a case study to be an empirical inquiry that "investigates a contemporary phenomenon in depth within its real-world context, especially when the boundaries between phenomenon and context may not be clearly evident" (p. 16). We argue that understanding risk appetite in an organization is dependent on the context, to the point where the boundaries between the phenomenon and the context is not clear. Since risk appetite is an integral part of an organization's ERM system, we find it necessary to study the phenomenon within the organizational context. Furthermore, we seek to gain in-depth

knowledge of how risk appetite is influenced and how it is institutionalized in an organization, and thus the case study strategy is preferable.

Third, a case study's unique strength is its ability to deal with a full variety of evidence and "benefits from prior development of theoretical propositions to guide data collection and analysis" (Yin, 2014, p. 17). As there is limited knowledge about our topic of interest, we need to use multiple sources of evidence when collecting the data in order to gain a rich understanding. This is especially important in answering the research questions since risk appetite is a concept that is challenging to investigate through interviews, archival data or surveys alone. The case study allows for triangulation between multiple sources of evidence (ibid). This is important as we acknowledge the need to let prior research on ERM, risk perception, and institutionalization guide our data collection.

We have chosen a single-case design for the following reasons. First, Yin (2014) warns that conducting a multiple-case study may require more resources and more time than what a researcher usually has at his or her disposal. In our case, we needed an in-depth understanding of the organizational context and how the organization has institutionalized risk appetite. In answering the research question, we need to dig deep into how actors in an organization rationalize their behavior, i.e. what determines appropriate organizational behavior for different risk categories. Without gaining a rich understanding of the organizational context, we would not be able to understand the data collection properly.

Second, we chose a study object that is interesting as a pilot case for analyzing risk appetite within our analytical model. In general, ERM is concerned with enterprise-wide risk management, and the intention is that the risk appetite should cover a broad range of risks. A pilot case would be to study risk appetite in a large organization with a wide risk exposure. However, Yin (2014) argues that the pilot-case argument for a single case, implies that the study is not complete by its own. In that regard, we encourage to include this pilot case in further research in the end of our thesis. Yet, our main contribution is to provide an analytical model for analyzing risk appetite in organizations.

Furthermore, we have chosen a case with multiple units of analysis, i.e. embedded single-case design (Yin, 2014). Since we are studying risk appetite through the lens of Scott's (2014)

institutional theory, we find a holistic single-case design to be too abstract. Since the intention of risk appetite is to align the organization with respect to how much risk to assume, we find it suitable to have two units of analysis, enterprise level and unit level.

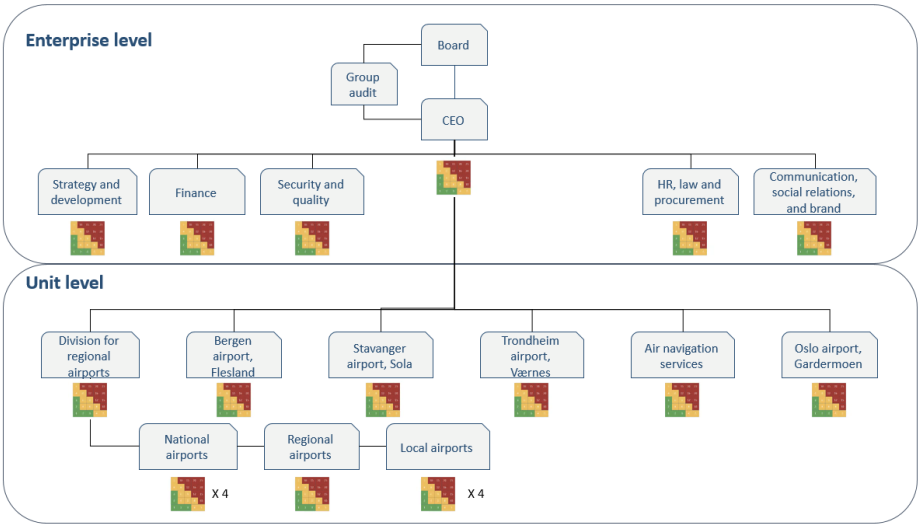
Study object: Avinor

The chosen study object for this thesis is Avinor, which is responsible for owning and operating a national network of 46 civilian airports across Norway. Avinor is also responsible for the joint national air navigation services for both the civilian and military sectors, and is organized as a state-owned limited company where all of Avinor's shares are controlled by the Ministry of Transport and Communications. Avinor's head office is located in Oslo, but the majority of the company's 3,157 employees are located at airports across Norway. Large distances, a dispersed settlement pattern, and challenging topography make Avinor's airport network an important part of Norway's communication infrastructure.

Over the past three years, Avinor has implemented ERM alongside strategic enterprise management. Avinor implemented these management systems to support decision-making in the organization and to increase cost and operational effectiveness. The two management systems was implemented in parallel, but the two systems are not integrated other than that top risks has been included in the balanced scorecards. Strategic enterprise management in Avinor is concerned with connecting key performance indicators with the strategic goals of the organization. ERM in Avinor is adapted from ISO 31000, and is concerned with identifying, evaluating, handling, and monitoring risks in the organization. One important difference between the two systems is that strategic enterprise management is essentially a top-down process, while ERM is mainly a bottom-up process.

Figure 5 illustrates Avinor's risk organization, and show how the bottom-up process of ERM works. Each division report a risk matrix, which is aggregated up to a joint risk matrix consisting of the most important risks from the unit and enterprise level. The joint risk matrix is not a mere aggregation of all the reported risks, but is a collation of the risks that are of enterprise-wide concern. Figure 5 also illustrates the two units of analysis in our case study of Avinor - the enterprise level and the unit level.

Figure 5 Avinor's risk organization



Avinor chose to implement enterprise risk management for different reasons. First, it was to support the achievement of Avinor's strategic objectives. Second, ERM was supposed to facilitate decision making in line with Avinor's risk appetite. Third, ERM was established to create processes for aggregation of risks and communication of risk management. Finally, Avinor implemented ERM to build and strengthen a holistic risk management culture (Avinor, 2014a). Risk appetite is a top-down element of ERM in Avinor. It is set on a strategic level in order to align the organization with respect to how much risk is acceptable to assume. In Avinor, the risk appetite determines what degree of risk exposure the organization considers justifiable and is contrasted to the risk exposure, i.e. the bottom-up feed, which is the collected probability and consequences of the risk Avinor is facing (ibid).

Avinor is a suitable case study for examining risk appetite. It is a large and complex organization in terms of the geographical spread of units. Additionally, Avinor's risk exposure is broad, ranging from safety risks, to commercial and strategic risks.

4.3 Data collection

The collection of data in case studies come from multiple sources (Yin, 2014). An important distinction to make, however, is between *primary* and *secondary* data (Saunders et al., 2009). In short, primary data comprise information that is collected or obtained for the purpose of the

research, whilst secondary data is information that have been collected by others for different purposes (Mehmetoglu, 2004). In the following, we explain how we collected empirical data for our thesis.

4.3.1 Primary data collection: Interviews

Since there is little data collected about what institutional pressures influence risk appetite and how it is institutionalized, we collected most of our data through interviews. Yin (2014) argues that interviews are excellent at providing explanations as well as perceptions, attitudes, and meanings. Furthermore, Yin (2014) argues that interviews within case research should resemble guided conversations rather than structured queries. Thus, we created semi-structured interview guides to guide the data collection towards relevant themes.

Saunders et al. (2009) describe semi-structured interviews as consisting of a pre-set list of themes and topics to cover, but that these may vary depending on the situation. By using semi-structured interviews, we have the possibility to ask follow-up questions during the interview and maybe uncover new sides and nuances to the research question. The flexibility of the semi-structured interview suits the explanatory purpose of our research, and is a common data-collection technique in case studies (Saunders et al., 2009).

We developed interview guides for the two different units of analysis, one for the enterprise level and one for the unit level. Johannessen, Tufte, and Kristoffersen (2005) depict an interview guide as an outline, where themes and questions make up the framework of the interview. The intention is to provide an appropriate structure to the interview and direct the attention of the interviewees to subjects that are relevant for the research question (ibid). The interview guides we made were thematically organized, and were focused on questions that were relevant for our chosen theories.

The interviews were recorded in order to make sure that no data got lost in the process of transcribing the interviews. Before starting the interviews, we asked the interviewees for consent to record the interview. Recording the interviews enabled us to actively listen and ask relevant follow-up questions during the interviews. In addition, we explained that we were not there to evaluate them, but rather to have their viewpoint on relevant topics of interest and not

necessarily the "textbook" or best-practice answers. The respondents and their answers were anonymized in order to allow the interviewees to speak more freely during our conversations.

In qualitative studies, the number of informants do not need to be as large as with quantitative studies, as the goal is to gain a deep understanding rather than a broad understanding of the subject (Johannessen et al., 2009). However, our respondents were all chosen based on their position in Avinor's risk organization, and our goal was to select informants who were well suited to answer our research questions. Saunders et al. (2009) call this purposive sampling, which is used when working with small samples, such as in case study research (ibid).

We chose informants from both units of analysis. We based our selection on the informants' positions and the responsibilities associated with those positions. We only interviewed informants who were mangers at the different levels, as these managers were close to enterprise risk management in Avinor. The enterprise risk manager at Avinor assisted us in booking interviews with the different managers, and Table 3 gives an overview of the respondents that were a part of the data collection.

Table 3 Respondents in Avinor

Level / role	Respondents	Interviews
Enterprise level	4	5
Unit level	6	5[3]
Total	10	10

4.3.2 Secondary data collection

During our case study, we also collected had access to some documentary data. For example, we collected several company presentations and internal documents on ERM. These documents helped our collection of primary data, as we were able to follow up with questions in the interviews about things we learned in these documents. Using this documentation, we were able to tailor our interview guides based on the roles and responsibilities in Avinor's risk management organization. An overview of the documentary data is found in the appendix.

[3] One interview was a group interview with two of the respondents

4.4 Data analysis

4.4.1 Research approach

Saunders et al. (2009) argue that is important to explain the approach used when analyzing the collecting data. Induction is concerned with building theories from data observed in the empirical world, while deduction makes forecasts based on existing theories, which empirical observations support or rejects (Arbnor & Bjerke, 2009).

In analyzing the collected data, we use an abductive approach. Lukka and Modell (2010) explain abduction as a process of oscillating between theory and empirical data in order to find plausible explanations to the problem of interest, while remaining open to alternative explanations throughout the process. Furthermore, Lukka and Modell (2010) argue that, "an important means of developing explanations in line with the pragmatist position is the process of abduction" (p. 467). Abduction harmonizes with pragmatism as it relies on the "skillful development of theoretical explanations with the help of everything that is known empirically and theoretically about the issue being examined" (Hanson, 1958; 1961 as cited in Lukka & Modell, 2010).

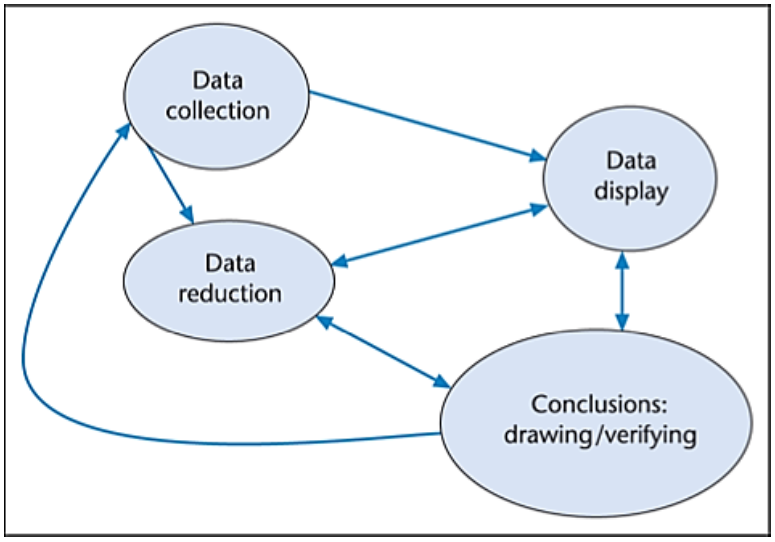
In practice, we started the research process with trying to get a broad understanding of what scholars, practitioners, and professional organizations had written about risk appetite. In this process, we developed assumptions about what factors may be important when institutionalizing risk appetite. After collecting data from interviews, we saw that we could not explain some parts of the overarching research question, and we needed to review relevant theory in trying to understand the issue at hand. As the data collection was done in several phases, we repeated this process as new empirical data was collected. Thus, there was an oscillating process of collecting data and reviewing existing research and theories about the subject.

4.4.2 Analysis

The figure below illustrates the process of analyzing qualitative data as suggested by Miles and Huberman (1994). The first stage of the analysis is to reduce and organize the collected data through coding or removing irrelevant data. The removal of data does not imply deleting it, but merely keeping the irrelevant data separate from the relevant data (ibid). The second stage is

data display, which implies providing an appropriate display of data, e.g. tables, graphical formats or networks (ibid). We are trying to display the organized data in a way that is manageable in order to draw conclusions from it. The last stage is conclusion drawing or verification, which implies drawing conclusions from the data set (ibid). As this process is repeated multiple times, it is also a process of verifying initial conclusions in order to see if they are consistent (ibid). However, as Figure 6 implies, there is not a strict order to these stages, and the process is interactive.

Figure 6 Data collection phase



(Miles & Huberman, 1994)

As the data-collection phase took several weeks, we repeated this process multiple times. After each round of interviews, we repeated the research question and the research objectives in order to have a consistent focus throughout the analysis. First, we read all the transcribed audio recordings while taking notes on observations that were relevant in a separate document. Second, we developed open-ended codes based on the notes we made. This meant to develop labels for "assigning units of meaning to the descriptive or inferential information complied during the study" (Miles & Huberman, 1994, p. 56). These categories made it easier to access and compare the collected data since we structured the data by topic, unit level and other relevant sub-groupings. Third, we drew conclusions through analyzing the organized data.

The findings from the data analysis are presented in two parts, as suggested by Corley and Gioia (2004). First, we present the first-order analysis, i.e. presenting the data in the language of the informants. In the first-order analysis, we try to avoid our interpretation of the empirical findings and let the quotes speak for themselves. However, the first-order analysis is structured thematically, based on which research question the empirical data relates to. Second, we provide a second-order analysis by assembling the categories into higher-order themes and analyzing them using relevant theory. However, the second-order analysis has deductive elements as we view the empirical findings through theoretical lenses and contrast them to previous relevant research.

4.5 Evaluation of chosen methodology

In general, much of the evaluation criteria of research have strong positivistic underpinnings, which favors quantitative research (Mehmetoglu, 2004). To apply the same evaluation criteria to qualitative research would treat a more subjectivist world-view unjustly (ibid). Even though there are many alternative ways of evaluating qualitative research (Creswell, 2007), scholars signify a failure to emancipate interpretive research from a positivist epistemology (Garratt & Hodkinson, 1998). Some scholars even argue that there is a "crisis of validity" in interpretive research (Gergen & Gergen, 2000). Lukka and Modell (2010) suggest that interpretive research can be validated by its capacity to include "both rich, emic accounts, grounded in profound understandings of the meanings of the researched, and explanations entailing an important etic and theoretically informed element" (p. 474). Furthermore, this validation is done across two central aspects, namely authenticity and plausibility (ibid). In the following, we discuss these central aspects in tandem since they are not mutually exclusive (ibid).

4.5.1 Authenticity and plausibility

On the one hand, authenticity refers to whether the researchers make an account that convince the reader that true emic understanding has been achieved from the field experience (Lukka & Modell, 2010). Authenticity is derived from the richness of the description and provide an emic account of the respondents' meanings (ibid). On the other hand, plausibility denotes whether relevant audiences can inter-subjectively accept the proposed explanations as sensible or likely (ibid). In order to increase the plausibility of an explanation, the researcher may apply credible theoretical knowledge in an abductive manner (ibid).

To convince the reader of the authenticity of our observations in the field, we have provided a rich and emic description of what level of risk is acceptable or unacceptable to assume from multiple informants, as suggested by Creswell (2007). Then, similar to Vaivio (2006), we developed a storyline of the emic accounts and then interpreted these against theoretical knowledge. Instead of integrating the emic accounts and the etic interpretations, we follow the suggestion of Gioia, Corley, and Hamilton (2012) to divide the emic account and etic interpretation into first-order and second-order analyses. The etic interpretation is a theoretically informed discussion where the emic accounts are analyzed through theoretical lenses. In chapter five, we provide the empirical findings by letting the "voice" of the respondents tell a narrative, while leaving out our interpretations. In that way, we try to increase the authenticity of our research by providing quotes from multiple respondents and accounts, as suggested by Creswell (2007). Such rich or "thick" descriptions allows the reader to make decisions regarding the plausibility of the subsequent explanations we present (ibid). In chapter six, we try to distance ourselves from the emic accounts and develop explanations through the application of theory and analytical tools, such as risk perception (Rosa, 1998) and neo-institutional theory (Scott, 2009).

However, the emic accounts may be biased due to poorly articulated questions (Yin, 2014). This is especially important in our case since risk appetite is not a part of the daily terminology of most respondents. We avoided direct questions about risk appetite but rather asked the informants about what determined the acceptable level of assumed risk in different risk categories[4].

The emic accounts can also be biased due to reflexivity (Yin, 2014), i.e. the interviewee gives the answers the interviewer wants to hear. We gave the interviewees a more general description of what we were interested in, and explained that we were interested in their subjective opinions on how the ERM system worked.

[4] See appendix for an example of an interview guide used in Avinor

4.6 Ethical considerations

Yin (2003) argues that it is important to discuss ethical considerations when doing case study research. The access we were given in Avinor required some level of responsibility from us as we could potentially get a hold of sensitive information. We signed an agreement that we were not to disclose confidential information that we might come across, and that we would behave according to the mandate that we had been given.

In accordance with Ritchie and Lewis (2003), we were careful to have the respondents' informed consent to both participate in the study and to record it. In addition, we provided the interviewees with information about who we were, what our purpose was, and how the data would be used.

As interviewers, we had to be aware of the "seductive quality" of our data collection method, which means that interviewees may appear comfortable and willingly disclose information that they may regret at a later stage (Ritchie & Lewis, 2003). To our understanding, this has not created problems during our research as we only met most of the informants once, and the informants were at a high level in the organization, i.e. managers. In addition, the respondents were asked to verify that the substance of the quotes we chose to include were correct.

5 Empirical findings

This chapter provides the first-order analysis of the empirical findings that we collected during the course of our research. The first-order analysis is organized thematically based on our two remaining research questions. First, we present the empirical evidence that relates to our second research question *what institutional pressures influence risk appetite in an organization?* Second, we present the empirical evidence that relates to our third research question *how is risk appetite institutionalized in an organization?*

5.1 Context

Avinor defines its risk appetite and manage its risks within boundaries set by important stakeholders. The government defines the overall scope of action for Avinor through its report to the national assembly on state ownership[5] every four years. In this report, the current government presents its ownership policy for Avinor based on recommendations that Avinor lays down in their §10 plan[6]. Operating outside of the boundaries drawn up by Avinor's owner is not a feasible option, as one member of top management explains:

> We are working with many of these things in the §10 plan, and that is to be passed in the national assembly, so that gives us many boundaries. To do things outside of that is unthinkable.

Corporate management in Avinor challenge the established operating boundaries drawn up by the government through Avinor's §10 plan, and try to negotiate on key strategic constraints. However, the owner always has the final say in these matters. Avinor has to accept and abide by these operating conditions, and it is within these constraints that Avinor articulates its strategic objectives and risk appetite. A member of top management explained how Avinor tries to challenge those constraints:

[5] Regjeringens eierskapsmelding for Avinor.

[6] §10 refers to the paragraph in the bylaws that requires Avinor to present their plans to the government in a report

> We are challenging this in the new ownership report to increase that limit. However, it is not a problem for us to accept those limits, and within those limits take a risk we can defend.

Avinor is self-financed, and does not receive funds through transfers from the government budget. With vast distances and a scattered settlement pattern, only a small number of the airports in the network generate a profit. As a results of this, larger airports cross-subsidize the smaller and often unprofitable regional and local airports. The enterprise risk manager explained how expanding capacity and increasing revenues at the two largest airports was important for the whole network as follows:

> It is a large network, and mainly four airports are profitable and finance the whole network. That is how we balance it, and by expanding at Gardermoen and Bergen. Get many passengers; get the airlines to want to land. Make ourselves attractive to the airlines so they increase the number of flights from our airports, and not at Copenhagen or Arlanda for example. That is extremely important for our whole funding of forty-six airports.

There comes a range of expectations with being a state owned organization. In Avinor, there is a strong pressure to keep within the acceptable boundaries and to behave in accordance with its owner's wishes. These expectations influence Avinor's willingness to take risks, i.e. their overall risk appetite. When Avinor broke with these expectations and became too aggressive on arrival duty free at one of its larger airports a couple of years ago, there was a political backlash and Avinor had to adjust its course. As one member of top management explained:

> […] it became a very political issue with the Minister for Transport and Communications in front, when passengers got duty-free bottles in the lap when arriving from abroad at [airport D]. Way too aggressive. They had to back down, remodel and so on, and then, you go too far. Even though business should be at the forefront, it has to be balanced in relation to our role and our owner.

Avinor enjoys a near monopoly position, as there are only a small number of privately owned and operated airports in Norway. However, there is an expectation from the owner that Avinor

must become more efficient, and there is considerable uncertainty about Avinor's future monopoly position. Deregulation and increased competition are possible consequences for Avinor if they fail to deliver on their mandated social mission[7]. For example, one member of top management explained how Avinor considers a long-delayed or mishandled opening of one of its large terminal expansion projects in Oslo and Bergen a considerable threat to Avinor's survival:

> It is not guaranteed that we can survive that as an organization. Then, someone might come and say that we cannot do this job, and that would challenge the whole model we are built upon. So, we have defined a few. If we do not deliver on our mandated mission, that is a critical risk that we put on our top list.

Avinor has delivered substantial financial returns back to its owner in the form of annual dividends to the treasury over the last years. There is an implicit expectation that they continue to do so. Because of this, there is a push not only towards financing the other airports, but also towards generating large surpluses for dividend purposes. As a member of top management expressed it:

> Our goal is that our company should offer more for less to society […] that we deliver steady and good results on all the areas that we are measured on, and continuously expand this for society. Additionally, if we can increase the returns to our owner through increased dividends and taxes that is also very positive.

Avinor's mandated social mission guides much of what it does, and it contributes to limiting how much risk is appropriate. A member of top management explained how Avinor is important to the public and how this was a change for him coming from the private sector:

> It was a new experience for me. Suddenly, what I am saying, what we do, is interesting for our society.

[7] Samfunnsoppdrag

Avinor has a mandated social mission, the annual report explains how Avinor is to "own, operate and develop a national network of airports for the civilian sector and joint air navigation services for the civilian and military sectors […] in a safe, efficient, and environmentally-friendly manner". For Avinor, this means that it does not have the power to reorganize or change the structure of its airport network without approval from its owner. As unit level manager explained:

> We cannot govern ourselves completely, because of this mandated social mission. Well, financially it would be beneficial to close down all of those forty-six, or at least twenty out of those forty-six airports, if we were to think purely in financial terms. However, there is that social mission that we are mandated to fulfill.

Avinor has historically had few incidents, and this safety culture is very prominent in the organization. As the enterprise risk manager explained:

> We have a strong safety track record. We are good at safety, and we have built that over many years.

The strong safety focus coupled with little commercial focus have contributed to Avinor being willing to take relatively little risk. One member of corporate staff explained how there has not been risk-taking culture in Avinor:

> I would say it is relatively low. There is not a culture characterized by a willingness to take risks. On the contrary, this was a government corporation, right. Rule-driven, influenced by bureaucrats that have had to develop more commercial insight, and that now becoming more commercialized.

Avinor does not feel the need to take large risks, and this has a moderating effect on Avinor's overall risk appetite. A member of the corporate staff expressed it like this:

> We are supposed to be a solid organization that does not need to take particularly large risks. However, we do challenge some thresholds, on duty-free for

> example, where we work up against political conditions that we come in conflict with. But, we are very wary. We do not take large risks, and we are very attentive towards the political environment.

5.2 Design

Avinor uses risk appetite, risk tolerance and risk willingness interchangeably in the steering documents on the ERM system. Risk appetite is the degree or level of risk exposure that Avinor considers justifiable or acceptable, and is set in order to align organizational behavior with respect to how much risk to take. Avinor's steering document on enterprise risk management defines risk appetite as:

> The degree of risk exposure the organization consider justifiable, where the risk exposure is the collected probability and consequences of the risk the organization is facing. The purpose of defining a risk tolerance, or the organization's risk willingness, is to clarify what is acceptable risk and what is not.

Furthermore, the risk appetite plays an important role in the steering document on ERM. The steering document puts risk appetite as an important part of one of its four purposes of ERM in Avinor. It states that ERM should "facilitate decision-making in line with Avinor's risk tolerance[8]". The rationale is that the ERM process should reduce the uncertainty of what risks the organization is exposed to by reporting risk exposure bottom-up. By better understanding its risk exposure, the organization can make better risk decisions and manage to operate in line with their risk appetite.

The risk appetite should guide the managing of risk in daily operations and guide both long term perspectives and strategic perspectives. As an elaboration of the second purpose, the steering document states that:

[8] Avinor uses risk tolerance, risk willingness, and risk appetite interchangeably in the steering document

> As such, Avinor can to a greater extent make informed decisions to handle risk in accordance with the enterprise's risk willingness. Both in day-to-day operations and in a strategic long-term perspective.

According to the steering document, Avinor's board and top management are responsible for setting the organization's overall risk appetite. Top management should define the risk appetite of the organization in cooperation with the enterprise risk manager, and the board is responsible for understanding Avinor's risk exposure and evaluate it up against the determined risk appetite.

The formalized risk appetite is set on a strategic level in the organization. However, respondents said that they had not formalized such a risk appetite in clear terms yet. Respondents said that this was because of the maturity of ERM in Avinor and that they had not gotten around to it yet. As one member of top management explained:

> This is where we have come the shortest. We have had this on the agenda. We have assessed risk appetite […] the more risk you take, the bigger the possibility to succeed is, and to profit in a way. Then the question is how far you want to stretch this. We have discussed this in the top management team.

Despite not clearly articulating a risk appetite statement in Avinor, the organization's appetite for risk is operationalized through guidelines and steering documents. It is reflected in the acceptance criteria for different risk categories, which indicate what scores on a scale from one to five to give during a risk assessment. The enterprise risk manager explained how the coloring in the risk matrix corresponded to risk appetite:

> That refers to the coloring in the matrix. What is supposed to be yellow, what is supposed to be red, and what do we mean by that. And we haven't gotten much further than that. It is not arbitrary if risk-factor ten is yellow or red. It has been assigned as an appetite.

Avinor has identified seven risk categories along with risk criteria for each. The main categories are strategic, supplier, financial, regulatory compliance, operation, HR, and infrastructure and

IT. Within each main category there are a number sub-categories adding up to a total of thirty-two categories in total.

All risks are assessed based on consequence and probability for it to happen, and the risk in question is given a score by multiplying consequence and probability. This provides the organization with a common language when discussing risks across the different divisions and activities. However, the criteria set by the enterprise risk manager indicate what level of impact is considered acceptable or unacceptable within the different risk categories. The assessments of probability are done within a three-year horizon and on a scale from one to five. Probability assessments are mainly subjective, while consequence assessments vary in how subjective they are, depending on risk category. Avinor acknowledges that risk assessments are subjective. As one company presentation reads:

> Assessments are done subjectively and thus depends on the available information and the experience of the assessor.

Once the evaluation of both the impact and the probability is done, the two scores are multiplied. The total score indicates where the risk is located in the risk matrix. If the product score is above 12, the risk becomes red and is considered unacceptable. Avinor defines red risks as:

> Risk beyond comfort zone. Mitigation measures must take place in order to reduce the risk level.

The coloring of the different product sums are intentionally set to reflect the overall risk appetite in the organization. The risk appetite is operationalized through the assigned colors for different product sums in the risk matrix. As the enterprise risk manager explained:

> We should have a conservative risk profile. We do not seek very high risks, but we need to accept risks in some areas. Therefore, the coloring should reflect that as well.

There is a two-way process in Avinor's ERM system. First, a top-down process of establishing guidelines for risk management, and second, a bottom-up process of aggregating the most

important risks. Risk appetite is determined at a strategic level and operationalized through the criteria that guide what score to assign the consequences and probabilities of risks in the organization (top down). Risks and risk exposure are aggregated and prioritized using the risk matrixes (bottom up). As the ERM steering document explained, ERM in the organization "[…] illustrates a two-way process: provisions and guidelines for risk management (top-down) and mechanisms for escalating the most important risks (bottom-up)".

Risk appetite seems to be a top-down concept in Avinor. It is set at a strategic level in the organization and is indirectly operationalized through guiding principles of how to assess risks. The color red in the risk matrix corresponds to a breach of the organization's risk appetite in that particular risk category. However, the risk exposure comes from a bottom-up process in the organization where each unit aggregates their risk profile and visualize the unit's top ten risks. Top management at the corporate level have to evaluate the aggregated risk profiles and give feedback on it. As the enterprise risk manager explains:

> Our CEO has internal board meetings, where he meets with management in Bergen. Among other things, Bergen tells about their risk management, and then our CEO has an opinion on that. "Okay, why do you have that so high on the list, and honestly, is that really how it is? What is the consequences and what mitigative actions are you planning?" So there is that one-to-one communication that way, and there is that whole [ERM] package.

When implementing ERM in Avinor, it was important that they did not bring in a new layer of external risk managers, but rather that they educated their own existing managers at the appropriate level. Existing managers could see the totality and understand the complexities of running an airport. Avinor felt that if the risk managers did not understand how the different areas of the organization was interconnected, then they would not make the right calls. As the enterprise risk manager explained:

> It was a point that we have a person senior enough to do a high-level assessment of the overall picture, but close enough to possess the expertise to catch nuances, right. It is a balance. If you are located too close to the runway, you are too far

> down, but an operating manager, a bit higher up, he might see a different complexity, and address the real issue.

5.3 Use

Avinor understands risk in terms of what can adversely affect the organization in the accomplishment of its objectives. However, the risk concept is wide, ranging all the way from operational to strategic and commercial risks. As one unit level manager explained:

> In a way, the risk concept includes everything from a screw falling out to the large financial risks. The strategic risks.

Safety and operational risks are an important part of Avinor's risk exposure. Aviation is Avinor's core business as an airport operator, and both national and international regulations govern most aspects of this industry. There are extensive regulatory frameworks relating to airport security, airside[9] safety, the environment, and health and safety. Risk management of such risks in Avinor most often follow a compliance based regulatory framework. As one member of top management explains, the consequences of not being compliant with regulations are large:

> You are either compliant, or you are not. And if you are not, the consequences are massive. If you're not compliant on security, you'll be defined as a "dirty" airport, and then everyone arriving from [Airport A] have to do a new security check when they land. Enormous consequences. It's very black and white. Either you are compliant, or you're not.

There are not just external regulations, but also extensive internal regulations. Numerous internal governing documents illustrate how regulations are an important part of Avinor's day-to-day operations. As one unit-level manager explained somewhat jokingly, albeit with a serious undertone:

[9] Airside references to everything that takes place in the air, on the runway, and the taxiway.

> We have 22,000 governing documents in Avinor. We have an ambition to have fewer, but traditionally we aren't very good at having few.

For large parts of Avinor, this rule-based approach to risk management is typical. However, mainly the largest airports manage more strategic and commercial risks. The enterprise risk manager explained this divide in the following way:

> That is the structure that exists in our organizational divide, where the operative layer, in large parts are driven by compliance and regulatory [elements]. However, the largest airports have some business and strategic elements in order to make the right decisions. There is a small mix, but the majority of the airports have mainly the regulatory perspective, in order to do things according to requirements.

Avinor has been, and still is, a very safety oriented organization. However, revenue from commercial activities has increasingly become more important as Avinor moves towards a more commercially oriented mind set. One unit level manager explained how the organization could increase its risk exposure without being irresponsible:

> We have been very focused on our inner workings, to operate safely, and all that. We are now moving towards operational streamlining and a more commercial mindset. I feel we need to take a little more risk. Not irresponsibly, but I think we have been a little reluctant, because we are focused on everything being so safe, and that holds us back, and it is expensive.

Deciding what level of risk is acceptable on commercial initiatives and activities is difficult, and there are not clear limits as to what is acceptable when it comes to strategic risks. This is because the criteria are ambiguous, as the enterprise risk manager explained:

> We have defined how much money is unacceptable, but only within some categories. For some risk aspects, it isn't crystal clear what our limits are. What we accept, and what don't accept.

For other types of risks, there are no direct guidelines as to what is acceptable, and only through discussion, can Avinor find out what much risk they are willing to assume. These discussions are somewhat detached from any explicit risk appetite, for example when considering a potential business venture. As one member of top management explained:

> So the discussion, are we to go into a joint ownership structure, or some other thing. Establish a company together, put assets in it, develop land and so on. Take it further, and increase returns. That is an ongoing discussion, but there is not an absolute [limit] that can help us in such a discussion.

In such discussions, it is challenging to evaluate these risks in relation to Avinor's risk appetite. For members of the organization, gut feeling, experience and a sense of what is acceptable decides how they assess many risks. As a member of corporate staff explained:

> In this instance, it becomes an analysis of the impact for my area, especially in relation to the strategy, and what is the likelihood for it to happen. Then you find out where this ends on the scoreboard, and in way, it is not an exact answer. It's subjective assessments that are done.

However, there seems to be a difference between the risk categories. A red operational risk is different from a red strategic risk. Red risks on operational activities demanded immediate mitigation measures, and that they would have to find ways in which they could reduce either the consequence or probability. A red strategic risk could attract attention from top management. A unit level manager explained:

> If you come from an operational risk assessment with red risks, that means that someone must do something immediately. I think that we adjust things on a strategic level to set focus. Something we have been doing more is, "here comes top management", and that [risk score] is actually green, but now it becomes yellow, because we want to discuss it.

Moreover, tweaking the end result of some risk assessments may unlock goodwill or resources. A unit level manager explained how there could be a strategic tweaking of the colors in their risk matrix:

> Strategically, it is smart for us to say that there is an issue here because we need goodwill or money.

Avinor also faces risks that are difficult to control, e.g. terrorism events, volcanic ash clouds, or airline strikes. There is little Avinor can do about those risks directly, other than to identify them and reduce the potential consequences. Safety is at the core of these considerations, and influences how Avinor thinks about these issues. Anything that could threaten the safety at the airport or passengers must be handled in one way or another. One unit level manager explained how they assess the potential consequences of such risks by looking at the potential impact for the passengers:

> How big a consequence does it create and who gets the consequence? Avinor has a strategy where the passengers are the ones in focus. If there are big consequences for the passengers, that is [the] determining [factor]. And then we are not talking about safety, because you do not pick on that anyway. Safety is the cornerstone.

Political decisions that might affect Avinor's operations in the future are important risks. Avinor cannot control these risks directly, but have to address them more indirectly by informing national, regional or local governments about the consequences of their decisions. One unit level manager explained how alternative use of land surrounding the airport could constrain future growth prospects:

> Another large risk category we have is land use around the airport. If the municipality, county or others open up for residential development close to the airport, that would limit our opportunities to expand and develop the airport. If we were not able to increase capacity, you would have to build a new airport some other place, and the needs of the region would not be covered. But that is a risk that we do not handle ourselves. There is a political and municipal side to

> it, as other authorities plan the regulative side of this. We need to flag these risks, and we have to work in the different forums to make the consequences of their actions visible.

The total risk exposure in Avinor consists of many different types of risk categories. Collating the different risk assessments is not an easy task for neither the unit level managers nor top management. As one unit level manager explained, collating the individual risks does not necessarily create a correct total risk exposure:

> The sum of all details does not equal the totality.

The bottom-up process of reporting risks in Avinor is not a mathematical aggregation of all the individual risk assessments. Each division or unit choose what top ten risks to include in their report and how the risk report should look like in the risk matrix. This process goes through two stages. First, each person who are responsible for a particular category, called risk responsible, evaluates his or her risk exposure by identifying potential threats and then evaluates the score based on an impact and probability assessment. Second, there is a plenary discussion of the identified risks in the management team. In these discussions, each risk responsible present their assessments and they discuss the assessments together. Only ten risks make it to the aggregate list, so there is naturally a discussion on what risks are the most important. Managers said that these discussions could be though as they try to achieve a consensus on their joint risk assessment. As one member of top management explained:

> It is more experience-based when we work with this. It is what the sum of competent people think, and that we agree on a decision. We can disagree initially, but we want to agree and own this together.

This first bottom-up stage is mostly based on the subjective assessments made by those who are close to and best qualified to evaluate the risks. The second bottom-up stage, however, could also be influenced by the social dynamic in the management group, as well as how they want to present their risk exposure to top management. As one unit level manager explained:

> It is okay that we have risk matrixes and all that, and that should follow the processes. But then again, it is a discussion about how we finally present these things, and how the enterprise risk manager sees this from the outside. It is one thing what we see internally, but what the enterprise risk manager sees from the outside is also important.

The risk report is influenced by how the management team would like it to appear in the eyes of top management. One unit level manager explained that they could not report too many red risks:

> We have this discussion in the management team, because we cannot have five risks that are red. There is something about your focus as well. Therefore, the debate on how to prioritize can be quite lively.

Respondents explain that there has been a learning process when it comes to how they are setting the criteria in the risk matrix. In the early phases, many reported red on all kinds of risks and there could be multiple red risks in the same unit risk matrix. The enterprise risk manager explained how they had to adjust things along the way:

> The coloring has been changed as well. We saw that, okay, we can live with this, we can live with more yellow [risks] than we had thought initially.

Reporting red on some key risks is a way of attracting attention from top management as well as holding focus internally. One member of top management explained how keeping a risk red could increase focus around an important project:

> What does red mean? In principle, it takes a product sum of probability and consequence to achieve red, and then the question is, do you use it to get focus on your own issues? Is red at [Airport B] the same as red at [Airport A]? The answer to that is probably no. We can have a different assessment than another airport, because it is not easily quantifiable. Do I flag something with [project name] to top management to make them focus on that? The answer is yes. Yes, I do.

Moreover, keeping a project on red after mitigation efforts keeps internal focus. Flagging a red risk and keeping it red, has a psychological effect on the division and creates a strong internal focus on the projects that really matter for management at unit level. As explained by a member of top management:

> A lot has been done, and it does provide a psychological effect to still keep it red. Both by saying that I am not yet content, or at the same time, you guys haven't done enough. Therefore, it can have two different effects. I have chosen to keep it red, until I have checked some things off the list. Then it might quickly go down to yellow and even green. The consequence is the same, but the probability is much lower. So, yes, sometimes I do use this deliberately so that the organization can keep focus on these things.

One manager at the unit level explained that there was room for them to adjust their end result to better fit how they collectively viewed their risk exposure:

> We are able to juggle this. We can adjust these risks up and down. We can on an issue-to-issue basis increase the probability based on a few parameters.

Respondents expressed that reality is more complex than what could fit into a risk assessment. Risk assessments were viewed as subjective and experience was brought up as an important factor in the risk assessment process. One member of top management explained that only risk assessments were not enough to understand the complexity of the risks the organization faced. As the member of top management explained:

> When you have that five times five matrix, I don't like that. In a challenging discussion, it is easy that it comes down to "Well, it is red, so that should have a higher priority than what is yellow". However, that isn't always right. Then you're too narrow-minded. You need to take a broader approach, lower your shoulders, and see that this is one of many tools to help you find out what to do, and how to prioritize. Sometimes, it is very easy to relate to red, yellow, and green. However, if you only use it like that, it is easy to oversimplify.

Once a unit reports their top risks, then the enterprise risk manager collate the different risk reports in cooperation with top management. Here, the top management have similar discussions. They discuss what risks deserve the attention of the whole organization and question some of the reported levels as well. It is a discussion of what the overall risk profile of the organization should look like. A member of top management explained:

> We discuss quite intensely. Where there are airports, divisions or companies that flag things, especially red. Either they want focus or resources. Then the question is, what is enterprise-wide enough?

When it comes to risk appetite and the defined criteria, top management discuss how to understand what is acceptable and what is not. One member of top management explained that one needed to look at the criteria and risks on an issue-to-issue basis:

> You need a push-pull mechanism on how you assess the risk in relation to the acceptance criteria you have defined. And that is an interesting discussion. In our discussion concerning risk in the top management team for example, you need to pull this in and out on an issue-to-issue basis.

Even though Avinor has tried to articulate acceptance criteria for some risk categories, it is not necessarily a goal to create criteria for every risk category. Acceptance criteria might not be valuable in themselves, rather discussions about and weighing risks up against each other is just as valuable. As the enterprise risk manager explained:

> It is difficult to define [criteria], and it might not be valuable to spend much time on that either. Comparing things against each other and correlate the risks, does perhaps achieve the same effect.

Risk appetite is not necessarily valuable for managing risk, but it could be valuable in the sense that it helps the organization to understand its risk exposure. Reporting red is a way of getting attention and make visible the different areas of the organization and making them aware of each other. The enterprise risk manager expressed this in the following way:

> And to visualize that the risk exposure is complex. “It isn’t just like this, it isn’t just like that, it’s actually more like this.” That is what we bring to the table, at least a possibility to see that we do not manage risk on a silo-basis. Not looking at the security and commercial environments separately, but that we see the two together. When you join the two, you get the possibility to create consensus and a common understanding from the two silos that you cannot prioritize that, because “look, instead we have to prioritize in this way”, and that clear things up a bit.

Discussions are an important part of risk practice in Avinor. Therefore, using the risk matrix to promote the views of different managers is not necessarily problematic. Rather, this use of the risk matrix makes a way for discussions about the nature of the risk exposure. As one member of top management explained:

> It is probably used by some to promote things they feel is important, but I think that’s okay, because it leads to meaningful discussions.

6 Discussion

This chapter is our second-order analysis of the empirical data presented in chapter five. In our first-order analysis, we presented our empirical findings by thematically organizing relevant quotes without interpreting them. In the following second-order analysis, we will view the empirical findings through the lens of theory and related literature.

6.1 Institutional pressures

Our second research question is *what institutional pressures influence risk appetite in an organization*? In answering this question, we draw on neo-institutional theory and the institutional pillars (Scott, 2014; DiMaggio & Powell, 1983) to explain how risk appetite is influenced by external and internal institutional pressures (Klovienė, 2012).

6.1.1 External pressures

We identified three institutional pressures – the ownership report, funding model, and state-ownership. We find that these pressures originated outside of the organization's control, which corresponds to external institutional pressures (Klovienė, 2012).

First, the organization's overall scope of action was defined by an ownership report. Even though the organization did try to challenge some of the boundaries drawn up in the report, respondents said that the organization would stay within the boundaries, and that it was not an option to go beyond what was included in the report.

The ownership report provides clear formal operating constraints for the organization. These constraints are formal and based on rules that the organization needs to accept or comply with. The report corresponds to the formalized rules and regulations that are indicative of the regulative systems' ability to constrain behavior (Scott, 2014).

There is a clear dependency, in the words of DiMaggio and Powell (1983), between the organization and its owner, stemming from the government's total ownership. This dependency allows the report to carry weight in the organization and provides grounds for a pressure to conform to the report.

Taking risks or engaging in activities beyond what is discussed in the report is not a feasible option for the organization. We find that the report has a moderating effect on the organization's risk appetite, and that this pressure to conform to the report is indicative of a *coercive* institutional pressure (DiMaggio & Powell, 1983) that is applied from the owner through the ownership report.

Second, the organization was self-funded, and only a number of the airports in the network were profitable. These airports cross-subsidized the smaller and often unprofitable airports. Respondents argued that the particular funding model gave the organization fewer possibilities to increase risk taking as the organization needed to keep a certain overall profitability, and a failure to fund the whole network could have large consequences for the organization.

The funding model was sanctioned through the organizational set-up and bylaws, and provided formal rules (Scott, 2014) that had a constraining effect on the organization's risk appetite. This lends credence to support the notion of the funding model being a *coercive* institutional pressure that is associated with the regulatory pillar (DiMaggio & Powell, 1983; Scott, 2014).

Third, the organization was subject to expectations stemming from being state-owned. Respondents explained that there were normative rules influencing the organization about how to behave as a state-owned organization, and that there was an implicit expectation to become more efficient, and pay steady dividends as the organization moved towards commercialization. The overall risk appetite was affected, as the organization did not want to take risks that might cause the organization to break with the normative rules as this created a sense of how the organization *ought* to behave.

Scott (2014) argues that normative systems define the means by which goals can be reached, and this corresponds well to an implicit expectation that a government owned organization should behave in a responsible way, be efficient, profitable and pay dividend back to the owner.

Normative systems can constrain behavior through a sense of what is appropriate behavior (Scott, 2014) and the organization not wanting to break with these expectations is indicative of a normative institutional pressure (DiMaggio & Powell, 1983). Scott (2014) argues that such normative systems may be coupled with a social obligation, that creates compliance to the

expectations in the organization. Therefore, we find that a *normative* institutional pressure (DiMaggio & Powell, 1983) stemming from external expectations have a moderating effect on the organization's risk appetite.

6.1.2 Internal pressures

Thus far, we have identified several external institutional pressures. As suggested by Klovienė (2012) we distinguish between external and internal institutional pressures by examining whether the pressure performs dependent upon a reaction from the organization. By looking at institutional pressures stemming from within the organization, we argue that organizational culture influence how much risk it is willing to accept.

The safety culture has its roots from both its socially mandated mission and its long history of mitigating risks. The mandated mission gives the organization an important role in Norway's communication network. Respondents emphasized the organization's role in society and its mandated social mission as important when asked about what level of risk that was acceptable in the organization. As an important part of society and the nation's communication network, the organization has developed a shared belief that what they do is not only in the organization's self-interest, but that they have an important role to play in society.

The owner externally mandates the organization's social mission. However, the social mission's importance in the organization seemed deep-rooted as it is a part of their organizational culture. Respondents repeatedly brought up the organization's mandated social mission as having a moderating effect on how much risk that was acceptable in the organization.

The organization has a history with very few incidents as a result of a strong safety focus. Respondents explained that the organization had historically been a rather bureaucratic government corporation that, because of its safety focus, largely had not been willing to take on risk in commercial activities either. This strong focus on safety has developed a shared understanding that the organization is conservative when it comes to risk. In other words, the organization's bureaucratic history creates a shared understanding of the organization as a "low risk" organization.

Shared beliefs and a sense of social obligation are indicative elements of the normative and cultural-cognitive system being dominant (Scott, 2014). It is difficult to pinpoint whether the normative or cultural-cognitive pillar is the strongest, but there seemed to be more of a common understanding about the organization's role rather than a social obligation creating the basis for compliance in the organization. This suggests that the cultural-cognitive system has the strongest influence (Scott, 2014) on the organization.

These shared understandings create a taken-for-grantedness (Scott, 2014) that moderate the overall attitude to risk and the risk appetite in the organization, and indicate the presence of a mimetic institutional pressure (DiMaggio & Powell, 1983).

The socially mandated mission, the organization's history of handling undesirable risks, and the low number of incidents influenced how the organization viewed risk as a whole. The organization was still dealing with leftovers from the previous bureaucratic and more rule-driven culture that gave the organization a low willingness to take risks. Therefore, we argue that the organization is influenced by a *mimetic* institutional pressure (DiMaggio & Powell, 1983) that has a moderating effect on risk appetite.

To summarize, we find that risk appetite in the organization is influenced by several institutional pressures that stem from within and outside the influence of the organization. Externally, the regulative system is influencing through formal rule-like procedures creating a *coercive* pressure on the organization, while the normative system is influencing through expectations about the organization creating a *normative* pressure. Internally, the cultural-cognitive system influences what level of risk that is acceptable through a collective understanding of their history and their role in society. This shapes the organizational culture, creating a *mimetic* pressure on the organization's risk appetite.

Table 4 summarizes the institutional pressures influencing risk appetite in the organization, by sorting the organizing the organization-specific pressures into more generalized themes.

Table 4 Institutional pressures that influences risk appetite

Pressures	External	Internal
Coercive	Formal rule-like procedures and regulations	
Normative	Expectations form stakeholders	
Mimetic		Organizational culture

The implication of these findings is that it is problematic to decouple the organization's risk appetite from its external or internal context. We find that risk appetite is influenced by, and specific to, the organization's context and cannot be articulated without taking into consideration this organization-specific context. To our knowledge, what determines and shapes the articulation of a risk appetite has not been addressed in the risk appetite literature. This finding implies that the articulation of risk appetite does not happen in isolation as a visionary statement, as implied by PwC (2014). Rather, both external and internal institutional pressures influence risk appetite. This further challenge the practicability of the risk appetite concept (Paape and Speklé, 2012) and the notion that it is a top-down concept (Power, 2009).

6.2 Institutionalization of risk appetite

In the following, we present the analysis of our third research question *how is risk appetite institutionalized in an organization*? In our analysis, we draw on neo-institutional theory (Scott, 2014), risk perception theory (Rosa, 1998) and Kaplan and Mikes' (2012) risk categories. We will answer the research question by analyzing the institutionalization of risk appetite through the two stages of institutionalization (Selznick, 1992).

6.2.1 Risk appetite in the ERM design – stage one

The first stage of institutionalization is characterized by a formal structure that provides explicit goals and rules in the organization (Selznick, 1992). We find that the first stage of institutionalization in our empirical case is through the design of the ERM system as the design states the *purpose*, *goals*, and *rules* for the ERM system.

The *purpose* of having a risk appetite in the organization is to make clear what level of risk the top management and the board consider acceptable. The risk appetite is concerned with stating what is acceptable for the organization's risk categories specifically and for the organization as a whole. Specifically, by setting risk criteria for each category for what is acceptable and what is not. Collectively, by reflecting the organization's willingness to assume risk in the coloring of the risk matrix. The *goal* of having a risk appetite in the organization is to align the organization with respect to how much risk to assume. The basic *rule* for risk appetite is that the bottom-up risk exposure is compared with the top-down risk appetite.

The first axis of our analytical model (as shown in Figure 4) is concerned with how subjective or objective a risk category is. In order to distinguish between these, Rosa (1998) suggests looking at how difficult it is to attain an inter-subjective agreement when discussing risk. In other words, if it is hard to agree about a risk claim, whether about its probability or impact, than that could be an indication of a subjective risk. In our empirical case, the organization have identified risk categories and set criteria for each of these. By doing so, the organization provides a common ground for understanding and discussing risk. This standardization of guidelines and risk categories suggest that the organization intend to make risk management more objectively understood. However, the risk appetite criteria are qualitatively given for many of the identified categories. Having such qualitative criteria suggest that some degree of interpretation is intended in the design. If we take in to consideration that the bottom-up risk exposure should be compared to the risk appetite, it seems that the organization considers the risk assessments to be somewhat objective.

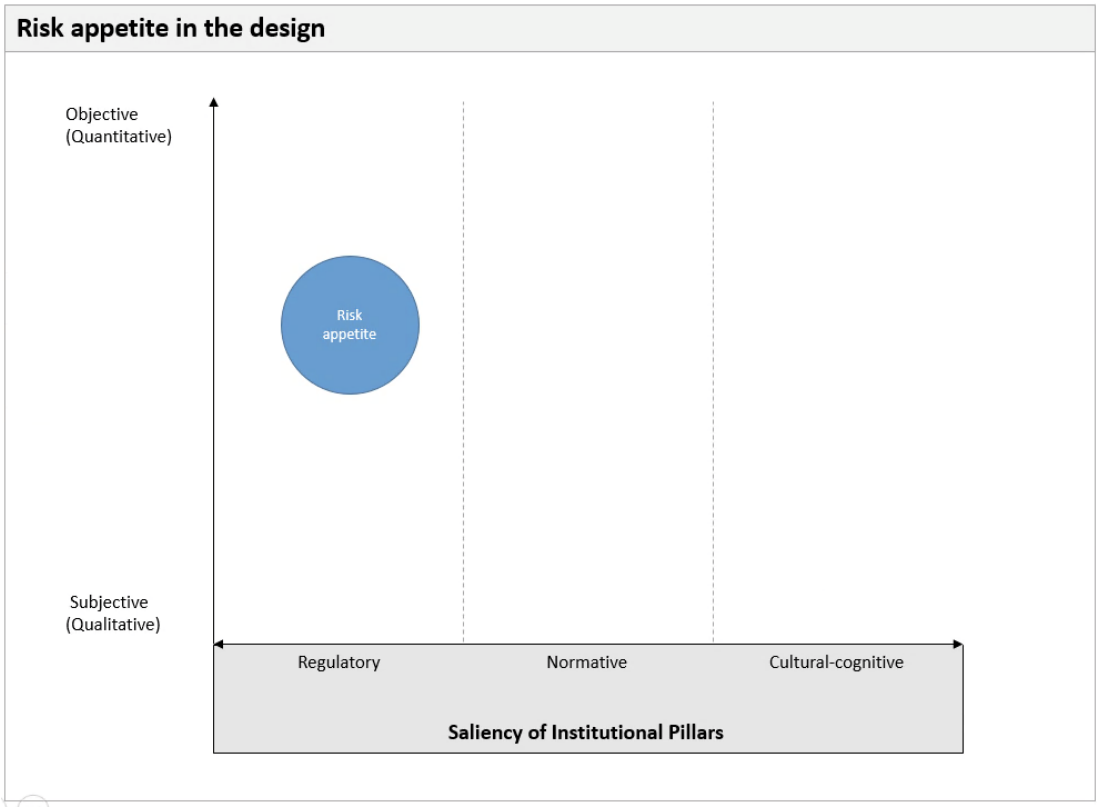
The second axis of our analytical model relates to what institutional pillars are the most salient or important in determining the acceptable level of risk (Scott, 2014). In our empirical case, the design provides the organization with rules and policies that both the enterprise and unit level have to comply with. The risk appetite is applied in the organization through criteria, that identifies when a risk is unacceptable and when it is not, and is monitored through the risk matrixes that the units report. Such rules and policies are indicative of the regulatory pillar, as the organizational actors have to comply with these policies in order to avoid sanctions (Scott, 2014). Risk appetite in the design seem to rely on coercive mechanisms for its behavioral effect. Coercion, as DiMaggio and Powell (1983) argue, can for example take place in a group where subsidiaries need to comply with policies of the parent organization. In our case, risk appetite

is an acceptance level that all units need to consider and report. If the report displays red, then there is a breach of what is acceptable to the organization.

The ERM system was implemented in an organization with a long tradition of handling and mitigating safety and operational risks. The concept of an overall risk willingness in the organization is therefore not entirely new as there has always been a strong risk management focus in the organization's industry. The organization has been subject to both regulative and normative mechanisms that have shaped previous risk management practice. There are many regulative mechanisms set by regulators that require a certain operational or safety standard. In addition, normative rules about high quality safety and operational procedures has previously shaped risk management in the organization. Risk mitigation is therefore deeply rooted in the organization, but the idea of having a risk appetite other than zero is relatively new. Risk appetite, in the sense that it is more than mitigating risks, is only found in the regulative design of the ERM system.

To summarize, we find that the institutionalization of risk appetite in the first stage is viewed more objectively as the organization intends to compare the bottom-up risk exposure with the top-down risk appetite. The first-stage of institutionalization relies on coercive mechanisms for its behavioral effect, which is within the regulative pillar (Scott, 2014). Figure 7 summarizes our discussion by placing the organization's risk appetite within the analytical framework based on our previous discussion.

Figure 7 Risk appetite in the design



6.2.2 Risk appetite in use – Stage two

The second stage of institutionalization is the process of making the formal rules, goals and policies a part of the social reality (Selznick, 1992). Institutionalization therefore, is not limited to the design in the formal documents. Rather, the institutionalization of risk appetite is concerned with what forces or motives that distinguish acceptable from unacceptable organizational behavior (Scott, 2014).

In our analysis of the second-stage institutionalization of risk appetite, we found that the respondents did not view all risk categories in the same way. Especially, respondents made a distinction between operational and safety risks, and other types of risks. Therefore, we analyze the second-stage institutionalization using Kaplan and Mikes' (2012) three risk categories; preventable risks, strategic risks, and external risks.

6.2.3 Preventable risks

Preventable risks are risks that arise from within the organization that does not offer any upside to the organization (Kaplan & Mikes, 2012). In our case, preventable risks were typically operational and safety risks, and the risk of being non-compliant with either international or national rules and regulations.

The first axis of our analytical model addresses how subjective or objective a risk category is (Rosa, 1998). In our empirical case, the risk appetite criteria set for preventable risks were not subject to much debate, even though the criteria were not always quantified. The respondents said a red score on a preventable risk was serious, and that there would be a need to initiate immediate mitigation efforts. The organization had much experience with handling and mitigating preventable risks, and there was a multitude of standardized processes for identifying, evaluating, and monitoring risks. Arguably, this could contribute to explain why there was a relatively coherent understanding of what red meant for preventable risks. The organization's experience and use of standardized assessment processes caused the discussions about preventable risks to be based on more objective standards and techniques. However, we found that the discussions about preventable risk assessment were concerned with probability claims. There were fewer standards for assessing the probability of preventable risks, making such claims more subjective.

In total, there was not much disagreement about preventable risks as there the organization had much experience with these kind of risks, making it rather objective in Rosa's (1998) framework. Yet, assessing the probability of preventable risks is dependent on subjective interpretations, which reduce the objectivity of the preventable risk category somewhat.

The second axis of the analytical model is concerned with the saliency of the institutional pillars (Scott, 2014), which is to say what mechanisms are important in distinguishing between unacceptable and acceptable risk. In our empirical case, we found that many of the organization's preventable risks were subject to national or international regulations that set the thresholds of what was required in order to be compliant. Respondents said that these were "black or white" considerations for the organization, where non-compliance was unacceptable. The organization had identified a "regulatory compliance risk" category that included risks

relating to compliance to regulations. For other preventable risks, internal standards and polices regulated what was acceptable.

In light of Scott (2014), the regulative pillar seems to be salient in shaping how much risk to assume for preventable risks. However, the institutionalization of risk appetite for preventable risks seems to be what Selznick (1992) calls “thick”, i.e. that the organization’s culture and norms support the regulative system to create compliance. In other words, the norms of the organization’s industry and development of a low-risk culture in the organization, support a low or non-existent risk appetite for preventable risks, but the regulatory pillar is by far the most important.

6.2.4 Strategic risks

Strategic risks are the risks that offer both an upside and a downside (Kaplan & Mikes, 2012). Despite not having a definition of risk that included both the upside and the downside, the organization has strategic risks such as financial risks, supplier risks, and infrastructure risks.

The first axis of our analytical model addresses how subjective or objective a risk category is (Rosa, 1998). For the strategic risks, respondents explained that the risk appetite criteria did not always provide a clear prescription for appropriate conduct. Since the organization had become commercially focused relatively recently, the organization had less experience with assessing and handling strategic risks and opportunities. Strategic risk assessments were perceived as subjective and the risk appetite criteria were not always clear to the organization. The frequent and often tough discussions about strategic risk assessment in the organization indicate that these risks were understood more subjectively (Rosa, 1998) in the organization.

The second axis of the analytical model is concerned with the saliency of the institutional pillars (Scott, 2014). Respondents explained that the risk appetite criteria for strategic risks were often vaguely understood. In contrast to the preventable risks, the regulative risk appetite criteria did not always distinguish between what was acceptable and what was unacceptable risks in the organization. Rather, through social interaction and discussions within the management teams, a shared understanding about what was acceptable and unacceptable developed. This common understanding of appropriate organizational behavior shaped what level of risk that was considered acceptable. The mechanisms that shaped what was the appropriate level of strategic

risks were mimetic (DiMaggio & Powell, 1983), which means that the organizational culture shaped what was the appropriate level of risk in the organization.

The organization had moved towards a more commercially oriented mindset over the last couple of years. Respondents explained how the organization in some areas ought to increase its risk exposure. There might be a normative pressure on the organization to increase its risk exposure as the organization moves away from its previous more bureaucratic mindset to a more commercial one. That the organization "ought to" increase its risk taking can be interpreted as sign of a social obligation that is indicative of compliance to a normative system (Scott, 2014)

For the strategic risks, a combination of the normative and cultural-cognitive pillar (Scott, 2014) determines what the acceptable level of risk is. We argue that norms implying that commercial organizations ought to take on more risk affect the organization. This serves as a starting point for the discussions in the management teams. However, through discussions within the management teams, a shared understanding develops about how much risk is acceptable in the organization. These discussions also occur between the top management and the different unit level managements. Through a bottom-up feedback loop, a shared understanding of the organization's risk appetite shapes what level of strategic risk the top management deems acceptable.

6.2.5 External risks

External risks are risks that arise from outside the organization's control and influence (Kaplan & Mikes, 2012). For the organization, the external risk category include a variety of risks ranging from volcanic ash clouds, terrorism events, and all the way to political decisions that could adversely affect the organization.

The first axis of our analytical model addresses how subjective or objective a risk category is (Rosa, 1998). Apart from compliance and regulatory elements concerning preparedness and routines, e.g. plans to handle volcanic ash or terrorism, the risk criteria for external risks does not always provide a clear prescription for what is acceptable.

Respondents explained that, often, external risks were placed in the risk matrix to voice a concern to the management team. For example, a political decision that could potentially limit future expansion opportunities for an airport was flagged in the risk matrix in order to create awareness about that particular risk. The organization could not handle these kinds of risks directly, but had to do thorough consequence analyses and work up against the different political actors to visualize the consequences for the organization of potential political decisions.

In our empirical case, discussions about external risks seemed to revolve around the assessment of probabilities and not the impact. Respondents did not say that it was hard to reach a consensus on the importance of an external risk. However, members of top management explained that they often challenged probability assessments, as units sometimes "overestimated" the probability for some external risks. This indicates that assessments about external risks included both subjective and objective elements.

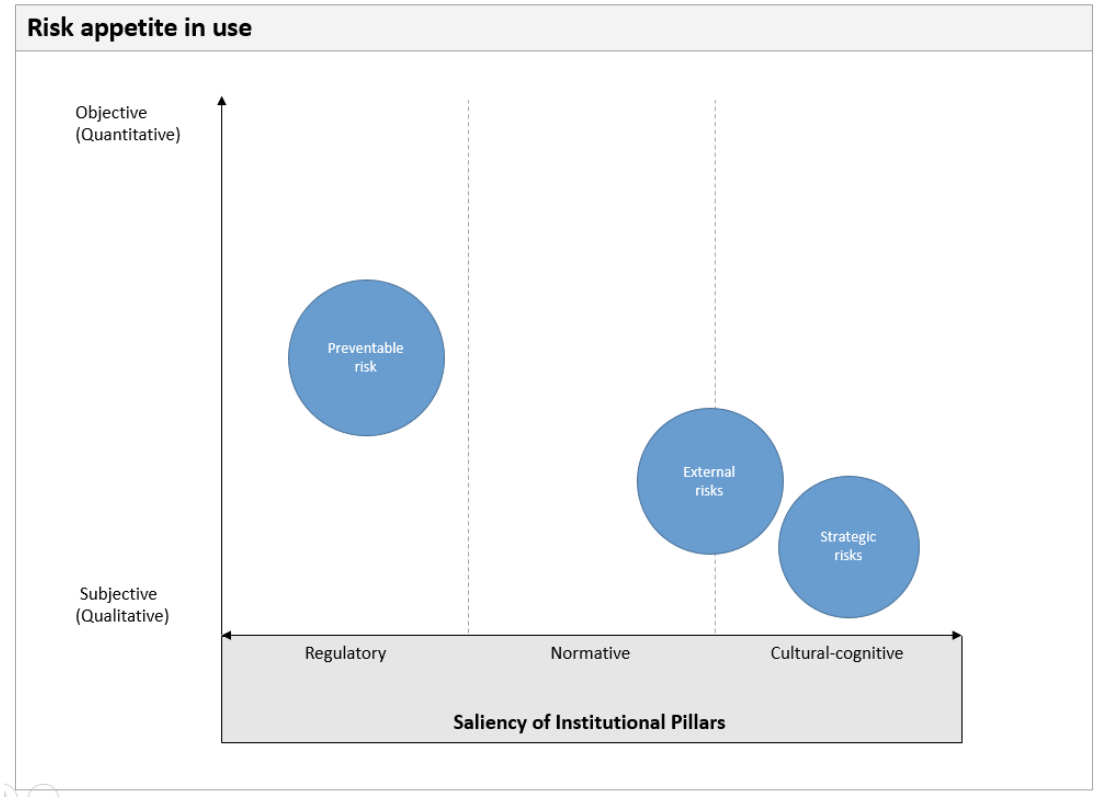
The second axis of the analytical model is concerned with the saliency of the institutional pillars (Scott, 2014). In our empirical case, we found that external risks could be many things as the risk exposure of the organization was varied. The regulative and normative pillars, as indicated by formal rules and international regulations, governed some of the external risks, while others, such as the risk of potentially unfavorable political decisions, were governed more by the organizational culture. Respondents pointed to the importance of strategic goals when determining what external risks to flag. Such shared beliefs are indicative of the cultural-cognitive pillar in Scott's (2014) framework.

There were many institutional pillars in play in determining what the acceptable level of risk was, as the external risk category was home to many different risks. However, beyond what was regulated by formal rules, we found that norms and organizational culture had the strongest influence. The acceptable level of risk was shaped by maintaining a good safety reputation (normative mechanism) and by the prevailing belief about what was of strategic importance in the organization (mimetic mechanisms).

To summarize, we find that the second-stage institutionalization of risk appetite varies across the risk categories. By analyzing the second-stage institutionalization, we find that the risk

categories varies in how subjectively they are understood. Figure 8 illustrates how we assess the organization's different risk appetites in terms of how objective or subjective the risk category is, and what institutional pillar is the most important in the institutionalization of risk appetite in the organization.

Figure 8 Risk appetite in use



6.2.6 Discussion about the institutionalization of risk appetite

The previous analysis of the first and second stage institutionalization of the organization's risk appetite reveal that there are three differences between them. First, we find that there is not just one risk appetite, but there are in fact several risk appetites in the organization. Second, we find that the risk appetite is more subjective for strategic and external risks. Third, we find that the acceptable level of assumed risk is to a large extent shaped by the cultural-cognitive pillar (bottom up) and not so much the regulative pillar (top down).

First, in our empirical case, we find that the institutionalization of risk appetite is different for the three categories of risk. In the design, risk appetite is the degree of risk exposure the organization consider justifiable, where the risk exposure is the collected probability and

consequences of the risk the organization is facing. This risk appetite design resembles risk appetite as defined in COSO (2004). However, the use of risk appetite is quite different. We find that that the organization intend to articulate a "clear" risk appetite, which is the collective probability and impact of the risks, but that there is not a clearly defined risk appetite in the organization. However, the different colors (red, yellow, and green) that are assigned to the scores in the risk reports functions as way of visualizing the organization's risk appetite.

In light of Power's (2009) argument that a singular risk appetite in an organization would be to over-simplify reality, we find that the organization interpret risks criteria differently depending on the risk category. For example, red on a preventable risk is not viewed the same as red on a strategic risk. As Kaplan and Mikes (2012) point to qualitative differences between the risk categories, we find that these differences also translate into different appetites for risks. This finding supports IRM's (2011) argument that there might be multiple risk appetites in the organization.

Second, we find that the risk appetite is more subjective for strategic and external risks. In order to discuss what might be the explanation for the increased subjectivity, we point to the discussions that the management teams have when they report their risk matrixes. First, the management teams discuss what top ten risks to report to enterprise management. Second, the management teams discuss what scores to assign to the different risks in the risk matrix.

In these discussions, respondents admitted that they adjusted the strategic risks in order to attract resources or attention. However, this was not the case for preventable risks, as they were understood more objectively. Adjusting the scores for the strategic risks could unlock goodwill or resources, as well as attention and internal focus.

Respondents explained that the sum of individual risk assessments did not necessarily create a correct picture of the overall situation in the organization. As a result, the management teams adjusted the risk scores, which represented how the management team understood their risk exposure. In light of Rosa (1998), this tweaking of some risks in different categories may indicate that that the strategic and external risk assessments are subjective, as they seem to depend on the social context.

Third, we found that the cultural-cognitive pillar is important in institutionalizing the risk appetites of the organization. In the design, the risk appetite was the top-down element of the ERM system that should guide the bottom-up risk exposure. In contrast to the design, we find that the bottom-up feedback influenced the organization's risk appetite and not so much the other way around. Respondents with responsibility for the setting of risk appetite admitted that the coloring of the risk matrix had changed as they learned more about the total risk exposure of the organization. Thus, it is not the top-down "risk appetite" with its guidelines and coloring that aligns the organization. Rather, the development of a culture and a shared understanding about what is acceptable institutionalizes an appropriate level of risk in the organization.

Scott (2014) argues that if a law or rule is sufficiently ambiguous, the law encourages collective interpretation, relying on more mimetic and normative than coercive elements for it to have a behavioral effect. In our empirical case, we find that the informants find it hard to understand the risk criteria if they are not quantified or explicit. In that sense, as the risk appetite criteria do not provide a clear prescription, the management teams try to collectively figure out how much risk they are willing to assume in a given category.

IRM (2011) argue that risk appetite needs to be measurable, to not become an "empty" concept. If we interpret "measurable" as "objective" in Rosa's (1998) framework, then a COSO-style risk appetite could rely on coercive elements for it to work effectively, i.e. through organizational rules and policies. If acceptance criteria are unambiguous, objective and quantifiable, they are also easy to monitor. However, to attain an "objective" risk appetite, we find that one cannot mix all categories of risk into one metric. The result of including both "subjective" and "objective" risks is to make the total picture more unclear and ambiguous.

Paape and Speklé (2012) argue that risk appetite set through formal criterions for different categories or objectives does not contribute to perceived risk management effectiveness. In this thesis, we have not addressed the effectiveness of risk management but how risk appetite is institutionalized. What we have found is that risk appetite set through formal criterions alone fail to address the importance of organizational culture and the unwritten norms in distinguishing between acceptable and unacceptable risks.

Power (2009) argues that risk appetite, as a concept, must be more concerned about human behavior and the dynamic process of involving a multitude of actors. We find that the risk appetite involves both individual and collective interpretations, as some risk categories are subjective. Moreover, we find that the "formal" risk appetite is not as important as the organizational culture in aligning the organization with respect to how much risk to assume. The risk appetite has changed over time, arguably because the organization "learned" more about how much risk it was willing to assume. This learning effect resembles what Scott (2014) calls, the emergence of a shared understanding, which is indicative of the cultural-cognitive pillar.

In other words, in the design, regulatory guidelines are set in order to institutionalize what level of risk the top management considers acceptable. These guidelines are acceptance criteria for all risk categories the organization has defined. However, when using risk appetite, the acceptable level of risk is not determined by the regulatory elements for all risk categories. For subjective risk categories, the normative and cultural elements are more important than the formal rules and policies.

7 Conclusion

In this thesis, we sought to answer the main research question *how do organizations understand their risk appetite*? To answer our main research question, we asked three research questions.

First, we asked *what is risk appetite*? We find that there is a consensus that risk appetite is the top-down element of ERM, but that the concept is defined in different ways. In large part, we find that the definition varies, but essentially carry the same meaning. However, some challenge the concept and do not share the same point of view. Furthermore, we find that risk appetite can be expressed both quantitatively and qualitatively, but there is a tendency to prefer quantitative measures. We find that the use of risk appetite has evolved in many directions, as it seems to be somewhat unclear how to implement risk appetite. In addition, scholars criticize the risk appetite concept for what they argue is a quantitative preference, for being vague, and impracticable.

Second, we asked *what institutional pressures influence risk appetite?* We find that risk appetite cannot be decoupled from its organizational, context as both external and internal institutional pressures influence it. Externally, formal rule-like procedures and regulations coercively influence how much risk the organization is willing to assume, while expectations from stakeholders shape the risk appetite through a normative pressure. Internally, a strong organizational culture supported by the organization's history influence risk appetite.

Third, we asked *how is risk appetite institutionalized in an organization*? We find that the design differed from the use in three different ways. First, we find that there are several risk appetites dependent on the different risk categories in the organization. Second, risk appetites differed in terms of how subjectively the organization understood them. The organization had less experience with some types of risks, which made their understanding of them more subjective. Third, we find that a bottom-up process contributed to determining what level of risk was acceptable to the organization, and to a lesser extent the top-down risk appetite. The top-down risk appetite is more effective in determining what is acceptable and what is not for more objective risk categories. However, when risk categories are more subjective, the policy driven and rule based risk appetite lost it behavioral effect as the norms and organizational culture became increasingly important.

To summarize, our findings shed new light on the concept of risk appetite. Most importantly, we provide a new way of analyzing risk appetite that can be applied in different organizational settings. We challenge the ERM assumption that risk appetite is only a top-down element. Our findings point in the direction that risk appetite needs to account for the importance of bottom-up processes through the organizational culture and norms, as the risk exposure is more subjectively understood.

7.1 Further research

This thesis is a pilot case, which may be included in a larger multiple case study of how to institutionalize risk appetite in organizations with different risk exposures. We encourage further research to be done in order to learn more about how risk appetite is institutionalized across different industries. By doing so, we could learn how risk appetite differs, in terms of institutionalization, for industries differing risk exposures. Even more research should be done to elaborate on what factors shape risk appetite in an organization. Furthermore, there is still much research to be done on how a top-down risk appetite affects decisions further down in organizations. In this thesis, we tried to understand how it shaped what level of risk that was acceptable at lower levels, and not so much how it affected actual decision making processes.

8 References

Arbnor, I., & Bjerke, B. (2009). *Methodology for Creating Business Knowledge.* London: SAGE.

Aven, T. (2013). On the Meaning and Use of the Risk Appetite Concept. *Risk Analysis., 33*(3), 462-468. doi:10.1111/j.1539-6924.2012.01887.x

Berger, P. L., & Luckmann, T. (1967). *The Social Construction of Reality.* New York: Doubleday Anchor.

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise Risk Management: Review, Critique, and Research Directions. *Long Range Planning, 48*(6), 265-276. doi:10.1016/j.lrp.2014.07.005

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise Risk Management: Review, Critique, and Research Directions. *Long Range Planning, 48*(6), 265-276. doi:10.1016/j.lrp.2014.07.005

Caldarelli, A., Fiondella, C., Maffei, M., & Zagaria, C. (2015). Managing Risk in Credit Cooperative Banks: Lessons From a Case Study. *Management Accounting Research. Advanced online publication.* doi:10.1016/j.mar.2015.10.002

Corley, K. G., & Gioia, D. A. (2004). Identity Ambiguity and Change in the Wake of a Corporate Spin-off. *Administrative Science Quarterly*, 173-208. doi:10.2307/4131471

COSO. (2004). *Enterprise Risk Management - Intergrated Framework. Framework.* Committee of Sponsoring Organizations of the Treadway Commission (COSO).

COSO. (2016). *About Us.* Retrieved May 31, 2016, from http://coso.org/aboutus.htm

Creswell, J. W. (2007). *Qualitative inquiry & research design: Choosing Among Five Approaches* (Second edition ed.). Thousand Oaks, CA: SAGE Publications.

Deloitte. (2014). *Risk appetite frameworks. How to spot the genuine article.* Deloitte. Retrieved May 2016, 20, from http://www2.deloitte.com/content/dam/Deloitte/au/Documents/risk/deloitte-au-risk-appetite-frameworks-financial-services-0614.pdf

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review, 48*(2), 147-160.

Douglas , M., & Wildavsky, A. (1982). *Risk and Culture: An Essay on the Selection of Technological and Environmental Dangers.* Berkeley, CA: University of California Press.

EY. (2015a). *Rethinking risk management. Banks focus on non-financial risk management.* EY. Retrieved March 1, 2016, from http://www.ey.com/Publication/vwLUAssets/EY-rethinking-risk-management/$FILE/EY-rethinking-risk-management.pdf

EY. (2015b). *Risk Appetite and Risk Responsibilities.* EY. Retrieved March 13, 2016, from http://www.ey.com/Publication/vwLUAssets/ey-risk-governance-2020-risk-appetite-and-risk-responsibilities/$FILE/ey-risk-governance-2020-risk-appetite-and-risk-responsibilities.pdf

FSB. (2013). *Principles for An Effective Risk Appetite Framework.* Financial Stability Board. Retrieved May 16, 2016, from http://www.fsb.org/wp-content/uploads/r_131118.pdf

Garratt, D., & Hodkinson, P. (1998). Can there be criteria for selecting research criteria? - Hermeneutical analysis of an inescapable dilemma. *Qualitative inquiriy*(4), 515-539.

Gergen, M. M., & Gergen, K. J. (2000). Qualitative Inquiry: Tensions and Transformations. In N. K. Denzin, & N. K. Lincoln (Eds.), *Handbook of Qualitative Research* (pp. 1025-1046). Thousand Oaks, CA: SAGE Publications.

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2012). Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methology. *Organizational Research Methods*. doi:10.1177/1094428112452151

Greenwood, R., Oliver, C., Suddaby, R., & Sahlin-Andersson, K. (Eds.). (2008). *The SAGE Handbook of Organizational Institutionalism.* London: SAGE.

Hansson, S. O. (2010). Risk: objective or subjective, facts or values. *Journal of Risk Research*, 231-238. doi:10.1080/13669870903126226

Hayne, C., & Free, C. (2014). Hybridized professional groups and institutional work: COSO and the rise of enterprise risk management. *Accounting, Organizations and Society, 39*(5), 309-330. doi:10.1016/j.aos.2014.05.002

Hoffman, A. (2001). *From Heresy to Dogma: An Institutional History of Corporate Envirnomentalism - Expanded Edition.* Stanford, CA: Stanford University Press.

IRM. (2010). *A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000.* London, UK: Institute of Risk Management (IRM). Retrieved March 5, 2016, from https://www.theirm.org/media/886062/ISO3100_doc.pdf

IRM. (2011). *Risk Appetite and Tolerance.* Institute of Risk Management. Retrieved February 15, 2016, from https://www.theirm.org/media/464806/IRMRiskAppetiteExecSummaryweb.pdf

IRM. (2016). *About The Institute of Risk Management (IRM)*. Retrieved May 31, 2016, from https://www.theirm.org/about/.aspx

ISO. (2009a). *ISO 31000:2009 Risk Management - Principles and Guidelines.* Geneva, Switzerland: International Organization of Standardization.

ISO. (2009b). *ISO/Guide 73:2009 Risk Management - Vocabulary.* Geneva, Switzerland: International Organization of Standardization. Retrieved June 4, 2016, from https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

ISO. (2016). *About ISO*. Retrieved June 4, 2016, from International Organization of Standardization: http://www.iso.org/iso/home/about.htm

Johannessen, A., Tufte, P. A., & Kristoffersen, L. (2005). *Introduksjon til samfunnsvitenskapelig metode.* Oslo: Abstrakt forlag.

Kaplan, R. S., & Mikes, A. (2012). Managing Risks: A New Framework. *Harvard Business Review, 72*(6). Retrieved February 5, 2016, from https://hbr.org/2012/06/managing-risks-a-new-framework

Klovienė, L. (2012). Institutional factors as criteria for business environment identification. *Economics and Management, 17*(4), 1245-1251. doi:http://dx.doi.org/10.5755/j01.em.17.4.2984

Knight, F. (1921). *Risk, Uncertainty and Profit.* Retrieved April 20, 2016, from http://www.econlib.org/library/Knight/knRUP.html

KPMG. (2008). *Understanding and Articulating Risk Appetite.* KPMG. Retrieved January 16, 2016, from https://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Documents/Risk-appetite-O-200806.pdf

KPMG. (2013). *Developing a Strong Risk Appetite Program. Challenges and Solutions.* Retrieved June 5, 2016, from https://www.kpmg.com/KY/en/IssuesAndInsights/ArticlesPublications/PublishingImages/risk-appetite-v2.pdf

Lukka, K., & Modell, S. (2010). Validation in interpretive management accounting research. *Accounting, Organizations and Society, 35*(4), 462-477. doi:10.1016/j.aos.2009.10.004

McKinsey and Company. (2012). *Enterprise risk management. What's different in the corporate world and why.* McKinsey & Company. Retrieved January 20, 2016, from http://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/working%20papers/40_whats%20different%20in%20the%20corporate%20world.ashx

Mehmetoglu, M. (2004). *Kvalitativ metode for merkantile fag.* Bergen: Fagbokforlaget.

Meidell, A. (2016). *A review and discussion of the influence and institutionalization of ERM: Achievements and future directions.* Norwegian School of Economics, Department of Accounting, Auditing and Law.

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

Mikes, A. (2011). From Counting Risk to Making Risk Count: Boundary-Work in Risk Management. *Accounting, Organizations and Society, 36*(4-5), 226–245. doi:10.1016/j.aos.2011.03.002

Miles, M. B., & Huberman, M. A. (1994). *Qualitative Data Analysis: An Expanded Sourcebook.* Thousdand Oaks, CA: SAGE Publications.

Olson, D. L., & Wu, D. (2008). *New Frontiers in Enterprise Risk Management.* Heidelberg, Germany: Springer.

Oltedal, S., Moen, B.-E., Klempe, H., & Rundmo, T. (2004). *Explaining risk perception. An evaluation of cultural theory.* Trondheim, Norway: Rotunde publikasjoner.

Paape, L., & Speklé, R. (2012). The Adoption and Design of Enterprise Risk Management Practices: An Empirical Study. *European Accounting Review, 21*(3), 533-564. doi:10.1080/09638180.2012.661937

Palthe, J. (2014). Regulative, Normative, and Cognitive Elements of Organizations: Implications for Managing Change. *Management and Organizaitional Studies, 1*(2), 59-66. doi:10.5430/mos.v1n2p59

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

PwC. (2009). *Risk appetite - How hungry are you?* PwC. Retrieved May 16, 2016, from https://www.pwc.com/gx/en/banking-capital-markets/pdf/risk_appetite.pdf

PwC. (2014). *Risk Appetite Frameworks. Insights Into Evolving Global Practices.* PwC. Retrieved February 05, 2016, from http://www.pwc.com/us/en/financial-services/regulatory-services/publications/assets/risk-appetite-frameworks.pdf

Quail, R. (2012). *Defining your risk appetite.* Corporate Risk Canada. Retrieved May 15, 2016, from https://erm.ncsu.edu/az/erm/i/chan/library/338_Corporate_Risk_Canada_Risk_Appetite_2012.pdf

Ritchie, J., & Lewis, J. (2003). *Qualitative research practice.* London: SAGE Publications.

Rittenberg, L., & Martens, F. (2012). *Understanding and Communicating Risk Appetite.* Committe of Sponsoring Organizations of the Treadway Commission (COSO). Retrieved January 9, 2016, from http://www.coso.org/documents/ERM-Understanding%20%20Communicating%20Risk%20Appetite-WEB_FINAL_r9.pdf

Rosa, E. A. (1998). Metatheoretical Foundations for Post-Normal Risk. *Journal of Risk Research*, 15-44. doi:10.1080/136698798377303

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research methods for business students* (fifth ed.). Harlow, UK: Pearson Education.

Scott, R. W. (2014). *Institutions and organizations. Ideas, interests, and identities.* Thousand Oaks, CA: SAGE Publications.

Selznick, P. (1957). *Leadership in Administration.* New York, NY: Harper & Row.

Selznick, P. (1992). *The Moral Commonwealth: Social Theory and the Promise of Community*. Berkeley: University of California Press.

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

Spira, L. F., & Page, M. (2003). Risk management. The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal, 16*(4), 640-661. doi:10.1108/09513570310492335

Tekathen, M., & Dechow, N. (2013). Enterprise Risk Management and Continous Re-Alignment in the Pursuit of Accountability: A German Case. *Management Accounting Research, 24*(2), 100-121. doi:10.1016/j.mar.2013.04.005

Vaivio, J. (2006). The accounting of "The Meeting": Examining calculability within a "fluid" local space. *Accounting, Organizations and Society, 31*(8), 735-762. doi:10.1016/j.aos.2005.12.007

Van der Stede, W. A. (2011). In the Wake of the Crisis: Some Reflections. *Management Accounting Research, 20*(4), 605-623. doi:10.1080/09638180.2011.627678

Woods, M. (2011). *Risk Management in Organizations: An Integrated Case Study Approach.* Abingdon, UK: Routledge.

Yin, R. K. (2003). *Case Study Research: Design and Methods* (Third ed.). Thousand Oaks, CA: SAGE Publications.

Yin, R. K. (2014). *Case Study Research: Desing and Methods* (Fifth ed.). Thousand Oaks, CA: SAGE publications.

9 Appendix

9.1 List of formal interviews

Table 5 List of formal interviews

#	Role	Function	Date	Length
1	ERM manager	Corporate staff	16.03.2016	65 min.
2	Director (1)	Top management	15.04.2016	50 min.
3	Finance director (1)	Finance	15.04.2016	55 min.
4	Safety and quality director (1)	Safety management	15.04.2016	65 min.
5	Director (2)	Top management	21.04.2016	65 min.
6	Finance director (2) Safety and quality director (2)	Finance Safety management	21.04.2016	65 min.
7	Strategic enterprise manager	Corporate staff	29.04.2016	55 min.
8	IT risk manager	Corporate staff	29.04.2016	55 min.
9	ERM manager	Corporate staff	29.04.2016	75 min.
10	Director (3)	Top management	29.04.2016	55 min.

9.2 Documentary material

Table 6 Documentary material

#	Name	Type
1	Enterprise Risk Management. *Helhetlig risikostyring. Ledelsdokument*	Steering document
2	Strategy for enterprise risk risk management. Enterprise policy *Helheltlig risikostyring - konsernpolicy*	Steering document
3	Changing the cultural paradigm. Enterprise risk management at Avinor	Company presentation
4	Enterprise risk management: Guiding principles for assessments *Helhetlig risikostyring: Veiledende prinsipper for vurdering*	Company presentation
5	Enterprise risk management. Categories and sub-categories *Helhetlig risikostyring. Kategorier og underkategorier*	Company presentation
6	Company plan 2016-2018 (§10 plan) *Plan for virksomheten 2016-2018 (§10-plan)*	Official report

9.3 Interview guide

The following is an example of an interview guide we used.

Introduction

1. About us and the project
    a. Short presentation about Joel and Håvard
    b. Short introduction to the master's thesis
    c. Anonymity
    d. Acceptance for use of recorder

2. General information
    a. The interview is anonymous and we want the individual's honest reflections and opinions about risk management in their organization, not textbook answers.

3. Background of interviewee
    a. What is your formal background/education?
    b. How long have you been with Avinor?
    c. Have you held other positions within Avinor before your current positons – if yes, what were they?
    d. Have you held other positions outside of Avinor? If yes, what were they, and for how long?
    e. What is your current position – what do you do?

Part 1: Risk management in Avinor

1. Very briefly, how was the transition from reactive issue management to proactive enterprise-wide risk management for you as a manager?
2. Risk process
    a. Risk assessment
        i. How are risk assessments done at the airport?
        ii. How formalized is this process? Guiding principles?
    b. Who owns the risks?
    c. Risk reporting
        i. Who reports what – and to whom?
        ii. How often do you report?
        iii. How do you report opportunities?

3. Risk and strategy
    a. How does the interplay between ERM and strategy work?
        i. Feed back both ways? (top down and bottom up)
        ii. In Avinor, what is the difference between strategic management and enterprise risk management?
        iii. KPI vs risk indicators

Part Two: Risk limits and perception

1. How would you define risk?
    a. What are your top risks?
        i. Are some of them more important than others? (relative exposure)
2. Risk assessment
    a. How do you reach consensus about what risks that are most important?
        i. Impact
            1. How do you determine the impact of a specific risk?
                a. Do you think of it as a relative consideration?
        ii. Probability
            1. How do you determine the uncertainty of a specific risk?
            2. What data is acceptable when determining the probability?
            3. How do you account for intuition or know-how in the risk assessment process? (subjective)
    b. Is it more difficult to reach a common understanding of some types of risks in terms of how they are perceived/understood? (O&R)
    c. How do you account for uncertainty? (surprises, black swans)
    d. Once you have determined these risks, how do you use them in the management team?
        i. Does it contribute to better management?
        ii.
3. **Risk reporting**
    a. What does it mean if someone reports red?
        i. Unacceptable compared to what? The strategic goal?
        ii. Do people use it to flag their concerns?
        iii. Is it a way of clearing themselves from responsibilities?
        iv. Does norms or culture play any part here?
        v.
    b. What makes a risk unacceptable (for example red) and where do this unacceptability come from?
        i. Declared risk profile/ Safety/HMS/Security/ Environment (preventable risks)
        ii. Paragraph 10 – plan (commercial initiatives) (Strategic risks)
        iii. Bankruptcies/politics/volcano (external risks)
4. **Risk limits**
    a. What implications do such limits have?
        i. Does it limit the scope of actions?
    b. What is you willingness to take opportunities when you see them? (opportunities)
        i. How is it encouraged by corporate management?
    c. What determines the acceptable level of total risk for your area of responsibly? (Risk appetite)
    d. In your opinion, what is the organization's appetite towards risk taking? (risk appetite)