The London School of Economics

and Political Science

The practice of Risk Oversight since the Global Financial Crisis: Closing the stable door?

Maria Zhivitskaya

A thesis submitted to the

Department of Accounting of the London School of Economics and Political Science for the degree of Doctor of Philosophy, London, September 2015

Declaration

I certify that the thesis I have presented for examination for the PhD degree of the London School of Economics and Political Science is solely my own work other than where I have clearly indicated that it is the work of others (in which case the extent of any work carried out jointly by me and any other person is clearly identified in it).

I warrant that this authorisation does not, to the best of my belief, infringe the rights of any third party.

I declare that my thesis consists of **68,728** words.

Abstract

This thesis examines the emergence of risk oversight since the global financial crisis, considering how different actors construct the idea of oversight and examining multi-level accountabilities that make it an organisational reality. The practice of oversight is assessed by 61 interviews and 17 weeks of field immersion in major financial institutions in London. The research questions are: 'How does the practice of risk oversight differ from management?', 'How has the concept of oversight evolved?', 'Where exactly within financial organisations does risk oversight happen?', and 'How do Risk Committee members operationalise their risk oversight role?' Tentative conclusions are also drawn on the extent to which enhancements in risk oversight since the crisis have strengthened financial institutions' ability to manage risk.

The first empirical chapter considers the evolution of regulatory attitudes to risk oversight before and after the financial crisis, and discusses the changing role of non-executives. The second empirical chapter on board risk committees discusses their accountability and relationships, both within and outside the firm. It shows board risk committee members to be an important part of the fabric of oversight who are still 'feeling their way' towards a stable definition of their roles and functions. The third empirical chapter discusses how oversight is organised within financial institutions. This is now commonly done through the 'Three Lines of Defence' framework. This is an idealised framework for risk governance that delineates how three layers of risk involvement (production, risk management and internal audit) are differentiated and also defined by their relations of oversight to each other. The last chapter discusses information intermediaries: the people within firms who create information flows within the oversight structures. Information is at the core of any oversight practice and this chapter shows that providing it to risk overseers, accurately and comprehensively, is a continuous struggle for the various parties involved.

CONTENTS

EXPANDED CONTENTS

Tables and Figures

Acknowledgements

First and foremost I would like to thank my supervisors Professor Michael Power and Dr. Matthew Hall for their continuous support and advice during the past four years, as well as the London School of Economics Accounting Department full PhD scholarship that made my research possible.

I am immensely grateful to the interviewees that were very generous with their time and the two firms that kindly allowed me to observe them.

A special thank you to Sir Howard Davies – I learned more from our conversations than I could possibly describe, and this PhD would not be what it is without his help in accessing interviewees.

I would also like to thank my parents and Tobias Prinz who were often more confident in me than I was. Thank you to David Kendix for the countless lunches and insightful discussions, and Sarantos Kaptanis for teaching me about academia and always being there for me.

Finally I am thankful to Andy Krasny, Victoria Tuomisto, João Oliveira, Jan Sramek, Kata Pfiszterer, Debra Ogden, Katya Radkovskaya, Dorothy Toh, Julia Morley, Daniel Polanco, Miguel Lim, Alistair DuPont, Julian Au, Nastya Zhvalevskaya and all the other people in my life who supported me in various ways throughout.

CHAPTER 1: INTRODUCTION

> "The growth of risk management is often stimulated by what appear to be its failures" (Mikes, 2011).

Despite its failures during the global financial crisis, recent years have seen an explosion of interest in risk management and risk oversight (Power, 2007; Arena, Arnaboldi, & Azzone, 2010) – "it is not an exaggeration to view risk management as one of today's most significant sense-making referents that actors use in the field to develop understandings of action and inaction" (Gendron, 2014). Risk oversight is "a defining feature of improving consistency in risk management" (Ashby, Palermo, & Power, 2012), but academics "are pointing to failures in the overall risk oversight processes" (Beasley, Frigo, Fraser, & Simkins, 2010).

What is risk oversight?

'Oversight' of risk is variously discussed in terms of macro-prudential regulation (Bernanke, 2008, 2011; Hanson, Kashyap, & Stein, 2010; Yellen, 2011), micro-prudential regulation (Carmassi, Gros, & Micossi, 2009; Goodhart, 2009; Herring & Carmassi, 2008), board-level oversight (Ho, 2012; Jalilvand & Malliaris, 2013; Leech, 2012; Spira & Page, 2003), and business unit level risk oversight (Bessis, 2011; Mikes, 2011; Miller & Waller, 2003) among other contexts. The purpose of this thesis is to access the practice of risk oversight via interviews and observations, and focus on how risk oversight is made real for and by different actors.

An in-depth exploration of the risk oversight phenomenon in the practice of large financial institutions in the UK is presented at the levels of (1) regulation, (2) boards, and (3) firms themselves. The study is supported by two 8 and 9 week-long field immersions and 67 interviews, mostly conducted in London.

London is an appropriate place to conduct this study because it is one of the world's two leading international financial centres[1] (ZYen, 2015), and was thus strongly affected by the global financial crisis of the late 2000s.

This thesis gives a top-down exploration of the practice of oversight: first from the regulatory perspective (primarily using document analysis), then Board-level oversight (based on interviews), followed by the 'Three Lines of Defence' (TLD)[2] organisational structures (based on regulatory and consultancy documents), and finally explaining Information Intermediaries (with the help of interviews within organisations). Chapters about Regulation and Organisational Structures (TLD) are more descriptive, while those on Boards and Information Intermediaries are more analytical. The combination of documentary and interview-based evidence allows a comprehensive discussion of risk oversight.

The empirical chapters are organised as two pairs of studies that shine light on each other: Regulators (Ch4) – Boards (Ch5), and TLD (Ch6) – Information flows (Ch7). These pairs belong to each other because boards are key actors in realising regulatory goals, and information flow processes are a way of operationalising TLD. Furthermore, boards oversee TLD with the help of information flows. Chapter 4 on Regulators and 6 on TLD are primarily based on analysis of documents and

---

[1] According to the 2013 ZYen Global Financial Centers Index - it has been ranked second after New York based on the 2014 and 2015 ZYEn Global Financial Centers Indexes.

[2] Three Lines of Defence is a frequently accepted framework of risk oversight in financial institutions: conventionally with business unit-level risk management considered the first line, independent risk management function second line, and internal audit third line. More detail in Chapter 6.

show an evolution of regulatory focus on boards and of TLD as an oversight structure. Chapter 5 on Boards and 7 on Information flows show the practice reality of those two areas, and are primarily based on interviews and observations.

1.1. Summary and Research Questions

The use of the relevant academic literature is an essential component of academic writing (Brodkey, 1987). Most of the academic background is given in in the second chapter, and the four empirical chapters include relevant academic references throughout, not as separate sections within each chapter.

After laying out the theoretical foundation (Ch2) and methodological tools (Ch3) to tackle the research questions, Chapter 4 presents an overview of regulatory developments and their historical context over the past three decades in the UK, which has particular relevance to the foundational aspect of practice, as it is then up to practitioners to interpret the guidance.

Chapter 4 asks, "*How has the concept of oversight evolved from the regulatory perspective? How does regulatory focus on risk oversight manifest itself?*" It presents an evolution of regulatory attitudes to corporate governance and financial regulation, and shows a convergence of these two strands of regulation around their interest in Boards and Board Risk Committees. This chapter also demonstrates an increased stringency of regulatory requirements that lead to a higher degree of responsibility Boards have for meeting them, that I describe as a process of responsibilisation.

Chapter 5, at the core of the thesis, looks into the meaning of the Board's oversight role, and asks "*How do risk committee members understand and operationalize their risk oversight role?*" Accountabilities and ambiguities that arise in the process are examined with the help of 15 interviews with Non-Executive Directors (NED[3]s), with a focus on how they understand their oversight role and how they balance a number of various accountability relationships (with shareholders, regulators, and management). Role ambiguity is a major part of this discussion, with a specific focus on directors' sense-making of how they operationalise their roles.

Chapter 6 asks, "*How is Risk Oversight operationalised at the organisational level?*" and demonstrates the practice of the "Three Lines of Defence" (TLD) risk oversight and management framework. Practitioner representations and interviews show that the framework imposes structures that allow some scope for interpretation by practitioners. The representations of framework are not decoupled, and practitioners are reacting to these representations: Power discusses "the significance of ideas and concepts in structuring practices", and asserts that "[i]deas are not something apart from practice - concepts and classifications are the ideational building blocks of the practice domain" (Power, 2007). Based on this assertion, one key principle that permeates this research is that since ideas are interlinked with practice, in order to truly understand the development of either, it is beneficial to look at both. Operational challenges are at the core of this chapter. Due to the pervasive institutionaliation of the risk management discipline (Power, 2004, 2009), models like TLD commonly attempt to describe the current state of the regime, but lead to a variety of possible modes of interaction between the practitioners across and within these lines, thus resulting in blurred boundaries.

---

[3] Note: Non-Executive Director is the UK term, while in the US the role is called an Independent Director. In the UK there can be NEDs who are not considered to be independent, e.g. former executives of the firm, or directors who have served a long term, but this practice is now discouraged and rare.

Chapter 7 examines the role of information flows in risk oversight process and asks "*How do the NEDs involved in Risk Oversight get the information they need?*" The chapter investigates the answer through two field observations and 46 interviews: it introduces and explains the role of information intermediaries who help link the whole system together by translating data into relevant information. This chapter demonstrates the interactive and iterative nature of information flows and breaks down the information process into the development, communication, and monitoring stages. It investigates practical manifestations of risk appetite and concludes that it is at the core of TLD because all these lines are ultimately defending the firm against the risk of exceeding risk appetite, with potentially costly consequences. This chapter is more speculative than the others, and raises a number of questions that could be addressed in more depth by future research.

The concluding discussion attempts to answer the question within the title of this thesis – namely can the recent enhancements to risk oversight and governance be fairly characterised as 'closing the stable door (after the horse has bolted)', or has it led to the establishment of a regime that is genuinely more robust and that, while not necessarily preventing another financial crisis, could at least be expected to make it less likely and to limit the damage caused.

CHAPTER 2: LITERATURE REVIEW

The realist approach to risk prevalent in economics or medicine, for example, treats risk as "objective, measurable, assessable and independent of the related social processes" (Andersen, Garvey, & Roggi, 2014). This thesis takes a social constructivist approach and implies that "practices and activities are seen as dangerous, or risky, through a process of developing shared meanings among people within an organisation or across a community" (Andersen et al., 2014), and indeed the way risk is viewed is influenced by organisational processes and actors. I use a similar approach to investigating board risk committees as Gendron did when examining Audit Committees as "constructed in the eyes of individuals who attend meetings" (Gendron & Bédard, 2006). The answers to the research questions, therefore, are descriptive of the actors' perceptions about their roles. This chapter explains which academic perspectives were chosen to shed light on the abovementioned research questions.

In "Organized Uncertainty" Power distinguishes between the construction of risk objects and the construction of risk management. The construction of risk objects "has a long tradition in scholarship which exhibits the considerable variety of ways in which risks become part of political and institutional agendas" (Power, 2007), while the construction of risk management is "a relatively underexplored theme in the risk management field" (Power, 2007). The focus of this study is not on risks themselves, nor on construction of risk objects (Hilgartner, 1992), but rather on organisational structures and processes that are in place to manage and oversee them, and on the people who do so and therefore shape their meanings. Power understands risk governance as "designs for the management of risk management" (Power, 2007).

"What we might call 'first-order' risk objects are increasingly subsumed within a model of management process, which in turn constructs them as 'auditable' risk objects" (Power, 2007). Not focusing on risks themselves allows to have an agnostic attitude to whether those 'first-order' risks exist and how they could be mitigated, and instead to focus on the second-order construction and oversight of those risks, as well as the actors' construction of meaning, in line with Bhimani's observation: "Concepts like risk and governance are ultimately social constructs shaped by the contexts they inhabit" (Bhimani, 2009).

A lot of the concepts dealt with throughout the thesis could be best understood within the context of their evasiveness and lack of clear definitions. To demonstrate, Andersen et al. (2014) observe:

> "Risk appetite, risk appetite framework, risk tolerance, risk culture, risk limits, and risk capacity are newer terms in the risk-taking lexicon that have come into vogue recently […] the precise meaning and metrics of these terms are evolving and thus there is still considerable inconsistency in their use" (Andersen et al., 2014).

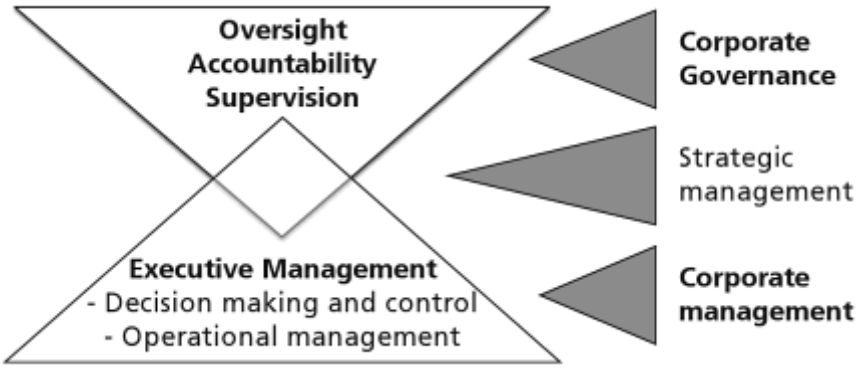
Despite the variation in the underlying meaning that different users might attach to these terms, these terms are commonly used – often without individual authors attempting to define them. Indeed, that equivocality is even true of terms such as 'risk' and 'risk management', because "it has been conceived and framed by different professional disciplines and theoretical traditions that see risk in certain contexts and through the lens of specific needs" (Andersen et al., 2014).

Corporate governance, despite being an ambiguous term itself, organises risk management and oversight:

> "Corporate governance considers the role of the board in its fiduciary role towards the official owners, the shareholders, and their obligations to fend off major disasters while optimising the value-creating potential of the enterprise" (Andersen et al., 2014).

The OECD researchers state that "Corporate governance involves a set of relationship between a company's management, its board, its shareholders and other stakeholders" (OECD, 2004). According to Cadbury, corporate governance is "a system by which companies are directed and controlled" (Cadbury, 1992), and according to Walker "The role of corporate governance is to protect and advance the interests of shareholders through setting the strategic direction of a company and appointing and monitoring capable management to achieve this" (Walker, 2009). Despite the numerous definitions of what corporate governance means, "there is a general agreement that governing a corporation and managing a corporation are distinct activities" (Andersen et al., 2014).

FIGURE 2.1: OVERSIGHT VS MANAGEMENT



Source: "Managing risk and opportunity", pg. 13 in Andersen et al (2014)

In Andersen's et al. representation of corporate governance, unlike management, governance is responsible for oversight and supervision: "Effective oversight of risk-taking is an important governance function and will remain a key responsibility of the board" (Andersen et al., 2014). In terms of governance structures, the empirical focus of the thesis is on oversight by the board risk committee, and on the risk management frameworks within the organisation itself.

"Oversight" is a broad term (Acheson, 2004), one which encompasses a wide range of activities and agents. One of the purposes of this research is to shed some light on this broad concept of oversight and show the ways it manifests itself in practice through the actors' sense-making. This chapter therefore explores the possible ways academic literature might help shape a framework that will direct this research towards finding the answers to those questions, as well as explaining the research methods used.

While investigating the literature, the goal was not to find how the term 'oversight' is used directly within different academic domains, but rather to identify literatures that focus on issues similar to oversight, and analyse how their discourses might be helpful to understanding how oversight is perceived and practiced by actors in the field. The objective of this chapter is thus to position the rest of the thesis within current academic debates and to draw out the relevance that these literatures have to understanding the practice of oversight.

As early as 1973, Stephen Ross explained that "Essentially all contractual arrangements, as between employer and employee or the state and the governed, for example, contain important elements of agency" (Ross, 1973). Agency theory makes an important contribution to accounting research and is central to accounting theory, following Kunz & Pfaff "[a]gency theory and its advocated view of the firm as a complex nexus of contracts constitutes one of the major pillars of theoretical accounting" (Kunz & Pfaff, 2002).

Agency perspective is particularly relevant to and useful for my research, because this thesis describes a number of complex explicit and implicit contractual arrangements between different levels of oversight within the financial sector – "levels of oversight" is an analytical term used in this thesis to describe the oversight relationships between regulators and the board (Chapter 4) at the highest level, between the board and managers (Chapter 5), and levels of risk oversight employees within the business (Chapter 6). Agency perspective is helpful in thinking about different levels of principal and agent relationships which interact with each other.

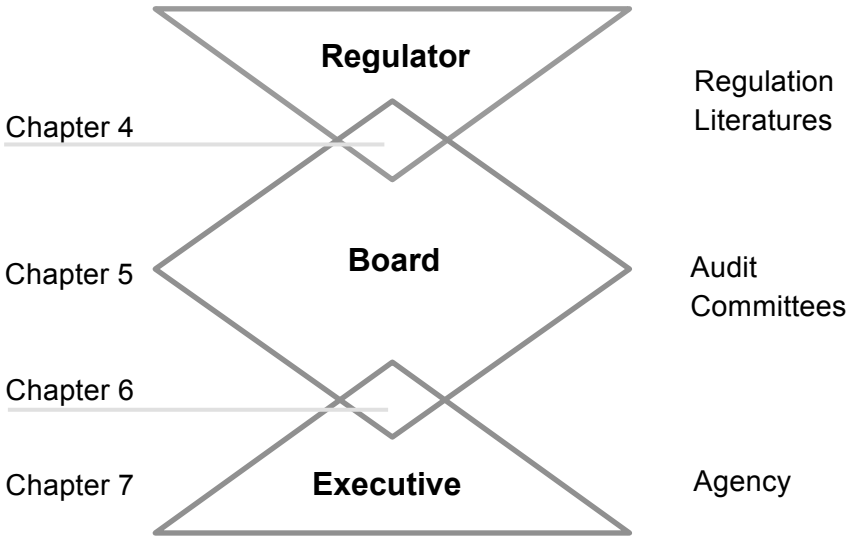
The agency perspective is used as an appropriate framework for understanding complicated interactions, while accepting its limitations as a concept whose origin lies in economic theory, and thus acknowledging that "agency theory models are not intended to be literal descriptions of the world" (Lambert, 2006). However, despite not giving a literal description of practice, agency theory provides a helpful broad framework for positioning the specific issues addressed in this research. And, additionally, I fill out and supplement this broad conception of the agency view-point with two strands of literature and thinking more directly relevant to the areas of study - the enforced self-regulation literature and the literature on audit committee effectiveness. In these settings agency theory is a helpful general perspective in understanding how the concept of oversight manifests itself in practice.

In his studies of oversight by audit committees, Gendron advocates "multivocality" (Gendron, 2009) and departure from typical uses of agency theory. Related to Gendron's suggestion, a theoretical framework used in this research in order to dissect and explain the components of oversight could include insights from two independent, but overlapping theories: agency and regulation. The research is also heavily rooted in the audit committee literature as a proxy that helps explain risk committees. A number of other theoretical frameworks could also have been appropriate, such as for example governance or management control. Regulation

and audit committee literatures were selected due to their direct fit with the empirical material about oversight.

Figure 2.2 is an adaptation of the Andersen's model to this research and demonstrates how the use of the abovementioned academic perspective is connected. In addition to the board (especially risk and audit committees) who oversee the firm's management, the role of the financial regulators and their oversight of the board is also considered. Agency language is used throughout the thesis in order to simplify the complicated relationships between varieties of actors; however contribution to the agency theory is not the objective of this thesis. Some of the relationships discussed have principal-agent attributes are: regulators – board members, board members – executives, executives – employees in their firms.

FIGURE 2.2: CHAPTER STRUCTURE OVERVIEW



Source: Own representation, inspired by "Managing risk and opportunity", page 21 Andersen et al (2014)

The literature review is organised the following way: first agency perspective is discussed because it is the foundation which provides a framework that will be used in every chapter throughout the thesis, and then elements of regulation and audit committee literatures are discussed, as the ones more accurately appropriate to the studies of regulation and board risk committees.

Chapter 4 investigates the 'principal-agent'- like regulatory oversight of the board, with a specific focus on the regulation of risk oversight. Regulation literatures are used in this section. Chapter 5 looks at the Board's role through the lens of Audit Committee literature, drawing the parallel between the Risk and Audit committees. Chapter 6 examines the governance framework within financial institutions, and the agency interaction between the managers and the board. Finally, Chapter 7 is about information flows and agents who operationalise it, therefore agency ideas apply most directly.

Due to the breadth and complexity of literatures covered, the discussion of the literature that follows does not aim to be comprehensive, but rather to help frame the reference points and methodological choices for a better understanding of the empirical phenomenon of oversight in a way that will aid understanding of oversight practice issues throughout the thesis. This chapter will demonstrate how application of these three academic research spheres shapes the questions on risk oversight and formulates the important issues addressed in this thesis: i.e. the practice of risk oversight in financial institutions with a focus on the UK experience. The thesis will, fundamentally, be treating oversight as an agency issue, and will apply the regulation and audit committee literatures as empirical subsets of the wider agency theme, as a way of better understanding the way actors' behaviours are shaped.

2.1. AGENCY PERSPECTIVE

> "The [agency] model is arguably the most popular model in use by accounting researchers today as evidenced by the body of extant accounting literature. […] Its basic propositions are easy to understand, intuitively appealing, and empirically tractable" (Cohen & Holder-Webb, 2006).

According to Kaplan and Atkinson, there are two principal-agent relationships in a typical firm (Kaplan & Atkinson, 1998): one is between the shareholders and managers (Jensen & Meckling, 1976), and another is at the institutional level - between top managers and individual divisions within the firm (Gupta & Govindarajan, 1991). Kaplan and Atkinson do not mention the Boards as intermediate layer of agency relationships. It is suggested, however, that a 'principal-agent' – like interaction between non-executives and the regulators is also a relevant one – despite not strictly working for the regulators, boards interact with regulators on behalf of the firm in making regulatory oversight possible.

Agency theory, as expressed above, provides a useful framework to think about the relationships within oversight framework; it is also a popular, well-developed and mature framework in accounting research. The structure of this section is as follows: firstly, the origins and definition of agency theory are mentioned, and then the key aspects of agency that are useful to the problem of oversight are described, specifically: information asymmetry and the problems arising from it, and the costs of overcoming that asymmetry.

2.1.1. BACKGROUND

Although agency theory was originally developed as an economic model[4] of behaviour (Jensen & Meckling, 1976; Ross, 1973), it has over time become a more general and widely accepted empirical phenomenon as evidenced by the analytical assertion that agency theory became an "industry that explores every permutation and combination of agency experience in the corporate form" (Shapiro, 2005). This agency experience is manifested by the fact that "[a]n agency relationship exists when one or more individuals (called principals) hire others (called agents) in order to delegate responsibilities to them" (Baiman, 1990). The term "hiring" is quite specific, but it is worth noting at this point that agency relationships can also be observed in most other manager-subordinate relationships.

Looking back to Eisenhardt as the starting point, the reason agency theory is relevant to the investigation of the phenomenon of "oversight" is that the agency problem "arises when (a) the desires or goals of principal and agent conflict and (b) it is difficult or expensive for the principal to verify what the agent is actually doing" (Eisenhardt, 1989). There are several oversight relationships that could be observed in the financial organisations, each of which has aspects of principal-agent interaction.

A primary way this research differs from standard agency theory, is that agency theory often describes the goals of the principals and agents as conflicting, and entails an assumption that portrays agents as lazy and purposefully elusive: indeed, "standard agency theory has often been criticized because of its

[4] For further discussion of economic foundations of accounting-related topics see: "Economics in Management Accounting" (Bromwich, 2006).

presumptions about human behaviour" (Kunz & Pfaff, 2002). While extent to which the goals of principals and agents diverge is not the focus of the empirical chapters, the focus here is on the nature of the interactions themselves, and on the places where these interactions happen in practice.

One of the assumptions borrowed from agency theory is that since there are a number of complicated information flows in the financial services institutions that make oversight happen, it is difficult or expensive to oversee and verify all the information used during the oversight process.

"Common to all principal-agent models is an information asymmetry assumption" (Baiman, 1990). Risk oversight provides a clear example of this information asymmetry in the agency relationship, because from the perspective of organisational design, oversight can be seen as being about agents giving appropriate information to the principals in order to help the principals execute their role. The agents have more information about the issue than the principals because they are closer to, and more directly involved in, the business process, but principals need this information in order to manage and monitor the agents well. This information asymmetry aspect of the theory is very relevant to accounting research, because accounting and risk management tools are a part of overcoming this problem.

And indeed, in relation to accounting research, some argue that "[a]gency theory has been one of the most important theoretical paradigms in accounting during the last 25 years. The primary feature of agency theory that has made it attractive to accounting researchers is that it allows the explicit incorporation of conflicts of interest, incentive problems, and mechanisms for controlling incentive problems into our models" (Lambert, 2006). Following that line of thought, this section demonstrates the specific aspects of agency theory that will be helpful to answer questions about oversight.

2.1.2. INFORMATION ASYMMETRY

Information flows and knowledge transfer between the agents and principals, as well as amongst the agents themselves, plays an important part in reality of the information asymmetry problem. Jensen and Meckling differentiate between specific and general knowledge, and define specific knowledge as "knowledge that is costly to transfer among agents and general knowledge as knowledge that is inexpensive to transmit. Because it is costly to transfer, getting specific knowledge used in decision-making requires decentralizing many decision rights" (Jensen & Meckling, 1995).

Furthermore, "[t]he cost of transferring knowledge depends on factors such as the nature of the knowledge, the organizational environment, and technology. […] Transfer, as we use it, means effective transfer, not merely communication. The recipient of knowledge is presumed to understand the message well enough to act on it" (Jensen & Meckling, 1995). Understanding effective information transfer, according to the actors involved, will be especially relevant to Chapter 5, as it looks at different functions of the risk management process within organisations, and Chapter 7 that investigates how information providers within firms help non-executives, who are likely to have more general instead of very specific knowledge, to perform their role.

Transformation of risk-related data into useful and relevant information that the 'recipients' such as management and boards can act upon is one of the key problems explored in Chapter 7. Information flows are central in setting business strategy: for example, Bhimani and Langfield-Smith find that "strategy development and implementation must be translated into tangible and identifiable activities to make them amenable to structured informational visibility" (Bhimani & Langfield-Smith, 2007).

Information asymmetry can create a so-called 'moral hazard' whereby "individuals engage in risk sharing under condition such that their privately taken actions affect the probability distribution of the outcome" (Hölmstrom, 1979), and might therefore take more risks since the burden is shared. Overcoming the agency problem is not merely about minimising information asymmetry and moral hazard, but also about the alignment of incentives monitoring practices associated with it (Andersen et al., 2014).

2.1.3. MONITORING

Another central problem in agency situations such as oversight is the cost of oversight in agency relationships, "It is generally impossible for the principal or the agent at zero cost to ensure that the agent will make optimal decisions from the principal's viewpoint" (Jensen & Meckling, 1976). This problem is especially significant in complicated financial institutions where both the number and the technical complexity of transactions are of such magnitude that only a few people close to these transactions might be able to understand them (and even then, might not understand them entirely). In such institutions, a considerable amount of information, as well as understanding its impact, might be private to certain groups of agents alone.

Since agency literature looks at incentivising agents, and functions under the premise that monitoring (observing agents' behaviours) and oversight (used here as a more active term, implying a possibility of modification in agents' behaviours) are costly and not possible to the full extent due to the information asymmetry. An underlying idea is that "The agent is assumed to have private information to which the principal cannot costlessly gain access" (Baiman, 1990). This insight is particularly relevant to Chapter 4 that discusses regulatory oversight of the firms, and Chapter 5 that investigates the corporate governance interaction between the

boards and the mangers. Hilb (2005) distinguishes between strategic and monitoring dimensions of corporate governance, and explains that strategic dimension could be most helpfully addressed with the use of stewardship and role theories, while agency and stakeholder theories are best for understanding the monitoring dimension (Hilb, 2012).

Simons characterises management control systems as "more than devices of constraint and monitoring: management control systems are the formalized procedures and systems that use information to maintain or alter patterns in organizational activity" (Simons, 1990). Therefore, according to this definition, information is not just a passive object that plays a part in the oversight process, but it also has an instrumental performative role in forming organisational behaviour. Chapter 6 discusses dome of the effects that information flows within the Three Lines of Defence organisational structure have on shaping the way risk oversight is operationalised in practice.

When exploring the agency issue empirically, one can observe a number of principals and agents; but their relationships are more complicated and multi-dimensional than classic agency theory allows: indeed, "Agency theory presents a partial view of the world that, although it is valid, also ignores a good bit of the complexity of organisations" (Bhimani, Ncube, & Sivabalan, 2015). Therefore the rest of this literature review is extended to include regulation and audit oversight literatures which are directly relevant to the thesis, and add a level of specificity to the wider agency approach that the thesis follows loosely without attempting to contribute to agency theory.

2.2. REGULATION THEORIES

The application of a principal-agent framework to the study of regulation, originally proposed by Loeb and Magat (Loeb & Magat, 1979) in the Journal of Law and Economics, allows examination of key aspects of the problem such as information asymmetry. Debates about regulation could be seen as having many fundamental overlaps with the agency literature: there are principals (regulators) who monitor the agents (regulated). Regulators themselves, however, are also agents acting on behalf of the government and the public.

This thesis treats regulators as proxy principals and does not deal with the "who guards the guards" problem in depth; the assumption here is of the benevolent regulator, i.e. the "regulator who seeks to maximise total surplus (consumers' plus firms' plus taxpayers') in society" (Laffont & Tirole, 1993)[5].

2.2.1. PRINCIPLES-BASED REGULATION

This thesis selectively uses certain aspects of regulation literature primarily in order to explain the changes in risk oversight imposed by micro-prudential regulators on firms. Furthermore, in later sections regulation theory explains the role of non-executive directors as pseudo-regulators: "Regulating the 'risk society' is a burgeoning academic and policy area and there are signs that existing systems of regulation, for example UK financial services, are coupling the correction of market failure with the management of risk as their organising principles" (Black, 2002).

---

[5] For an exploration of the problem of the self–interested regulator see parts V and VI of Laffont (1993).

Focusing on UK-based financial institutions and regulators, the two useful concepts are principles-based and risk-based regulation (Baldwin & Black, 2008; Baldwin, Cave, & Lodge, 2010; Black, 2004; Walker, 2009). These two concepts help demonstrate the way micro-prudential regulation[6] evolved over time: e.g. Baldwin et al in The Oxford Handbook of Regulation explain that "Principles-based regulation, and in particular its associations with firm judgment and with industry guidance, has strong resonances with the self-regulation techniques which enrol market actors in the regulatory process and which are a longstanding but disputed feature of regulatory landscape: […] financial market regulation in recent years has seen a move away from self-regulation and towards greater centralization" (Baldwin et al., 2010).

The mechanism of micro-prudential regulation is based on the assumption that the regulators issue rules (which create mandatory binding obligations) and guidance (which explains how to comply with the rules and is non-binding) relating to the desired behaviour by the firms. These rules and guidance are used by regulators who oversee how firms comply with all of them, bearing in mind that should the firms not comply, they may be punished. Regulatory oversight thus manifests itself at the end of the regulatory process, where the corrective action taken as a result involves telling the firms to alter their behaviour: regulatory oversight could therefore be seen as a form of externally influencing the firm's own management process.

[6] Macro-prudential regulation looks at the way firms interact with each other in financial markets and create the potential for systemic risk, while micro-prudential regulation focuses on the capital soundness of individual financial institutions.

2.2.2. ENFORCED SELF-REGULATION

The concept of 'Enforced self-regulation' (Baldwin et al., 2010) adds to agency literature because it "characterizes the potentially cooperative relationship between regulator and regulated" (Power, 2007), where regulatory activities then focus on the "oversight of the self-regulatory activities" (Lodge, 2014). Therefore, when regulators allow organisations to self-regulate, they need to determine a way of seeing into each organisation in order to enforce this self-regulation and to check how the organisation self-regulates. This gives internal control systems, a special case of self-regulation, "a central role" (Power, 2004) and means that firm-focused research helps to understand the practice of enforced self-regulation. While it might seem that it is at the opposite end of the spectrum from any governmental regulation, Sinclair argues that there can be a "spectrum of coexisting policy choices" (Sinclair, 1997). According to its proponents, self-regulation is a more responsive and context-driven kind of regulation (Schulz & Held, 2004), and might result in regulated institutions being more prone to "buy into" the ideas and thus avoid regulatory arbitrage (Fleischer, 2010). Those who oppose it base their arguments on the "powerful distrust of profit seeking private enterprises regulating their own business activities" (Omarova, 2011).

In order to develop their own systems for compliance with the rather vague definitions of a self-enforced regulatory regime, financial institutions increased the size of their internal compliance functions and hired external consultants (Power, Ashby, & Palermo, 2013). While the loose definitions and requirements given by the regulators could have led to a variation in the level of compliance, these variations might have been flattened out and made more uniform by the presence of consultants (e.g. the consultancy arms of the big 4 accounting firms) who have a strong influence on the process of interpreting and 'translating' regulatory requirements.

Omarova observes "Amid widespread, and largely justified, scepticism toward banks' and other financial institutions' ability to act in a socially responsible or publicly minded manner, a call for allowing them to run their own affairs is

counterintuitive", but argues that what is needed is a new self-regulatory regime "which would focus explicitly on the issue of systemic risk prevention and impose the responsibility of protecting the public from financial crises directly on the financial services industry" (Omarova, 2011).

The enforced self-regulation approach "requires organizational self-regulatory arrangements to be verifiable. There must be a regulatory correlate visible and auditable at the organization level – and this is how the internal control system has become a key resource for this kind of regulatory style" (Power, 2013). Due to the strong emphasis on the internal risk regulatory mechanisms, enforced self-regulation "could be seen as a form of subcontracting regulatory functions to private actors" (Hutter, 2001). The role of the government can be seen in that case as "regulation of self-regulation" (Schulz & Held, 2004) or "meta-regulation" (Black, 2001).

This thesis looks at the regulation of risk at the entity-level within financial institutions and at the corporate governance that is in place to support the risk management and oversight processes. Hood et al observe that risk regulation regimes entail three components: "standard setting, information gathering and behaviour modification" (Hood, Rothstein, & Baldwin, 2001); in terms of the practical implementation of this pattern, regulators need the support of businesses in order to provide them with information required for oversight.

The currently mandatory Basel capital framework requirements "encourage financial institutions to develop more effective internal risk management practices by allowing them to rely on their internal models for measuring the riskiness of their assets" (Omarova, 2011). In fact, Power observes "The self-control activities of organisations have become an essential component of regulatory agendas" (Power, 2004). Enforced self-regulation is an underlying theme of the risk oversight discussion throughout this thesis, because while the first line of defence (see Chapter 6) self-regulates, the board (see Chapter 5) needs a way of looking at it and getting information which will allow it to see what is happening and allow it to choose where to intervene, should it deem it necessary to do so. In this way boards could be seen as similar to the regulators, since they share many elements of

functionality, and philosophies coming out of regulation theories can be used to characterise the activities boards engage in as they oversee management. As transmitters of self-regulation between the firms and regulators, non-executive directors are heading risk oversight within the firms, and crucially both they and the regulators are relying on information intermediaries within the firms (Chapter 7) in order to make it possible.

Regulatory interactions with the board risk committees will be discussed in Chapters 4 and 5. The next section focuses on the literature that is mostly directly helpful in understanding boards and the board risk committees.

2.3. Corporate Governance and Audit Committees

There are many definitions of corporate governance, but there is a "general agreement that governing a corporation and managing a corporation are distinct activities" (Andersen et al., 2014): i.e. the governing actors of a corporation are the shareholders (or board members who act as their representatives) who provide "oversight, accountability, and supervision" (Andersen et al., 2014) while executive management takes control over the operations and daily functioning. This leads to the creation of an inherent principal-agent relationship between the shareholders (often a large widely dispersed group) who act as the principals and who are usually not insiders, despite providing the financing, and on the other hand the managers and employees who know more about the firm. While the limited liability nature of listed firms naturally "reduces the security enjoyed by lenders and provides incentives for increased risk taking on behalf of shareholders" (Spira & Page, 2003), corporate governance systems aim to solve this ingrained principal-agent conflict between the shareholders and their agents within the firm. Accountability mechanisms, such as "financial reporting, internal control and audit" (Spira & Page, 2003) facilitate risk management within the corporate governance framework, enabling boards to act on behalf of the shareholders to address the collective action problem.

Corporate governance literature conceptualises the role of the board in various ways, focusing e.g. on the board's role to monitor (Fama, 1980) and control (Baysinger & Hoskisson, 1990) management in the classic agency sense where management is seen as opportunistic and it is thus the role of the board to protect shareholder value; or to support (Huse, 2007) managers who already intrinsically want to do a good job (Donaldson, 1990) in the stewardship theory sense (Donaldson & Davis, 1991). Daily et al explain that stewardship theory serves "both as a complement and a contrast to agency theory" (Daily, Dalton, & Cannella, 2003). Spira and Bender compare and contrast the work of audit and remuneration and discuss the tension between strategic and monitoring aspects within the NED role on these committees - they find that these roles are not as strictly opposed to each other as some commentators suggest. They also note that "Structure and composition of board sub-committees can be mandated: conduct and relationships cannot" (Spira & Bender, 2004).

Roberts et al. study work and relationships of the non-executives though in-depth interviews and find that this traditional theoretical distinction "between agency and stewardship theory, and control versus collaboration models of the board do not adequately reflect the lived experience of non-executive directors and other directors on the board". To solve this mismatch between theory and their findings, they use "accountability as a central concept in the explanation of how boards operate" (Roberts, McNulty, & Stiles, 2005). 'Accountability' is interpreted as an aspect of the principal-agent interaction, where boards are accountable to a number of entities including the regulators.

Roberts et al find that "the role of the non-executive is to both support executives in their leadership of the business and to monitor and control their conduct" (Roberts et al., 2005): this point leads to a question about the level of involvement that NEDs need to have within the business which is discussed in Chapter 5. Developing that further, "The contrast of oversight and support poses an important concern for directors and challenges them to maintain what can become a

rather delicate balance" (Daily et al., 2003), thus the boundaries of the NED role are a relevant focus of research.

2.3.1. Boundaries of the Board Risk Committees

Gieryn explains "demarcation" as "ideological efforts by scientists to distinguish their work and its products from non-scientific intellectual activities. The focus is on boundary-work of scientists: their attribution of selected characteristics to the institution of science […] for purposes of constructing a social boundary that distinguishes some intellectual activities as "non-science"" (Gieryn, 1983). Chapter 5 shows the way NEDs define their oversight role on the boundary between risk oversight and risk management. Mikes applies Gieryn's work on boundaries (Gieryn, 1983) to the realm of risk management practice and distinguishes risk experts based on their approach to calculative cultures. They can be divided into two camps: either quantitative enthusiasts or quantitative sceptics. Mikes states that "experts try to define what is and is not their remit, often with respect to competing or complementary fields of expertise" (Mikes, 2011). Based on that observation about role definitions and on the fact that risk and audit are often spoken about together, investigation of the audit committee literature can be a helpful way of thinking about risk committees.

Spira and Bender observe that in the UK "The establishment of board sub-committees has been strongly recommended as a suitable mechanism for improving corporate governance, by delegating specific tasks from the main board to a smaller group and harnessing the contribution of non-executive directors" (Spira & Bender, 2004). These committees typically include an Audit Committee, Risk Committee, Nomination Committee, Remuneration Committee, etc. The focus of this thesis is on risk oversight as conducted primarily by risk committees, but as discussed in Chapter 5.

Mikes explains that "'professions' originally emerged as a demarcation problem, i.e. a problem of boundaries between "special" and ordinary occupations" (Mikes, 2011), and shows that while Abbott (Abbott, 1988) looks at the actual characteristics of the professions that make them different from others, Gieryn uses the notion of boundaries (Gieryn, 1983) to "emphasize its rhetorical, discursive nature: how does group X define itself through descriptions of how they are *not* like groups Y and Z?" (Mikes, 2011). According to Zietsma and Lawrence, boundary work researchers have focused either on "professional/occupational boundaries" (Abbott, 1988; Zietsma & Lawrence, 2010) or "ways in which actors work to establish coordination across boundaries" (Carlile, 2002; Zietsma & Lawrence, 2010). The Three Lines of Defence framework involves separate groups coordinating various tasks and working together: business units, risk managers, and internal auditors. The way their roles are defined and operationalised is discussed in Chapter 6.

Boundary-work focuses on actors' definitions of their roles in relation to others: what is it that they do that the others do not? But confusion in boundary work might result in role ambiguity: e.g. Kahn et al. (1964) defined role ambiguity as a "lack of necessary information available to a given organizational position" (Kahn, Wolfe, Quinn, Snoek, & Rosenthal, 1964), which can be extended to mean "a concept that explains the availability of role-related information" (Ahmad & Taylor, 2009). Chapter 5 investigates the NEDs' self-perceived role ambiguity both in terms of the scope (what falls under the realm of the Risk Committee) and depth of involvement.

2.3.2. AUDIT COMMITTEES

Gendron and Bedard observe in 2006 that "The audit committee (AC) is one of the main corporate governance mechanisms upon which are predicated stakeholders hopes in constraining the behaviour of corporate managers" (Gendron & Bédard, 2006). They advocate for qualitative studies of audit committee (AC) effectiveness and explain that "macro perspectives on AC effectiveness can only provide meagre insights on a variety of fundamental issues such as: the way in which attendees of AC meetings make sense of AC effectiveness; the extent to which meanings of AC effectiveness differ significantly across attendees; and the way in which these meanings are produced" (Gendron & Bédard, 2006). Methodology chapter that follows explains the way the same principle has been applied to studying risk committees and the organisations they oversee, keeping in mind the concepts of accountability and oversight as constructs of the actors who perform them.

The earlier increased focus on the oversight responsibilities of audit committees has been discussed widely, often as a relationship between the audit committee inputs and financial reporting outputs[7]. Beasley et al. interviewed 42 members of board audit committees, and framed their findings as a tension between tension between the agency theory "view of the audit committee as an independent monitor of management versus the institutional theory view that audit committees may often be primarily ceremonial in nature, with a focus on providing symbolic legitimacy but not necessarily vigilant monitoring" (Beasley, Carcello, Hermanson, & Neal, 2009) – they found that "members strive to provide effective monitoring of financial reporting and seek to avoid serving on ceremonial audit committees".

[7] See "The Audit Committee Oversight Process" (2009) by Beasley et al for an overview

Gendron and Bedard (2006) find that audit committee effectiveness is constructed through "ceremonial features of meetings", "reflective interpretations of the substance of meetings" and "reflective interpretations of informal practices" (Gendron & Bédard, 2006). When studying oversight and construction of accountability, the separation between ceremonial and reflective features can also be relevant. Gendron and Bedard's paper "focuses on the micro-production of meaning within the small circle of people who attend AC meetings. We did not examine how meanings of AC effectiveness are constituted beyond this circle, in the eyes of outsiders" (Gendron & Bédard, 2006). 'Micro-production' of meanings of oversight and accountability, is also the focus of my study. However, the research object here – oversight – is explored not just from the way it is constructed by the board members (Chapter 5), but also from the perspective of regulators (Chapter 4), and risk governance frameworks within the firm (Chapter 6).

Beasley et al. show that "the extant literature largely fails to examine the process used by audit committees as a whole or by individual audit committee members when fulfilling their oversight responsibilities" (Beasley et al., 2009). This finding was also confirmed in a comprehensive literature review in 2010, when Bedard and Gendron reviewed 103 audit committee studies, and one of the key areas missing is related to the process dynamics surrounding Audit committees. Taking these observations into account and assuming that risk committees are similar to audit committees in that "AC members' capacity to play their monitoring role depends, in large part, on the quality of the information they receive" (Bédard & Gendron, 2010), this thesis extends the view beyond looking at information from the perspective of the receivers into also researching the suppliers of information, and the process that information goes through in Chapter 7.

2.4. CONCLUSION

Agency perspective is used throughout the thesis as a reference point in understanding the risk oversight interactions, but the aim is not to contribute to agency theory itself, but rather to use it to see how oversight plays out in practice.

This chapter has explained three areas of literature used to construct the academic framework for the empirical findings that follow. Oversight is seen primarily as an agency problem, so the agency perspective is examined as the broadest conceptualisation of oversight relationships. Agency presents a general framing resource to the problems of oversight. Making it more specific, the aspects of regulation theory highlighted could also be seen as a subset of the agency problem – for example, enforced self-regulation involves regulators enlisting parties they regulate in helping them perform their role. Regulation literature is used as a particularly focal reference point when illuminating the increasing regulatory focus on individual responsibility in relation to risk oversight in Chapter 4.

Narrowing the focus further towards the board risk committees, one of the main areas of research in this thesis, parallels are drawn with the literature on audit committees. Audit committee literature is discussed because of the assumption that despite the differences that will be explained in Chapter 5, a lot of the knowledge about audit committees will be transferrable to the less researched domain of risk committees. Underlying aspects of agency relationships will be discussed throughout the thesis, but more precisely Chapter 6 will focus on corporate governance and Chapter 7 on information problems.

The chapter has demonstrated how this project could be situated in relation to other bodies of literature; agency literature is treated as a useful broad framework, and regulation literature makes agency theory more descriptive of the empirical phenomenon of oversight in practice. Audit committees make the comparison with risk committees even more direct.

To conclude the brief literature overview, this thesis uses elements of agency as a useful framework and a point of orientation rather than explaining oversight as a pure agency problem or attempting to contribute to the agency theory. Oversight is costly and could be simplified into the interactions between principals and agents. As demonstrated above, adding regulation literatures allows us to unpack the concept of oversight and give richness to agency theory. The following section deals with the consideration of social science research methodologies appropriate to address the research questions, and describes why these methods were chosen in order to add depth that formal agency models cannot achieve.

CHAPTER 3: METHODOLOGY

3.1. INTRODUCTION

A frequently voiced concern in management accounting literature is the 'relevance gap' between research and practice (Aram & Salipante, 2003; Pettigrew, 1997; Roberts et al., 2005). Hall notes that "Accounting research, and management research more generally, has been criticised for becoming far too removed from the practices and activities it seeks to investigate and illuminate" (Hall, 2010). This thesis seeks to bridge the gap between research and practice by basing research on practitioner sense-making about the field and their roles – therefore rooting theory observations in findings from the field.

A number of authors have urged accounting and management researchers to adopt qualitative approaches (Ferreira & Merchant, 1992; Vaivio, 2008). The broad objective of this research is to understand the concept of 'risk oversight' as operationalised by practitioners, and a decision was made early on that using qualitative research methods would be the most appropriate way to address the questions involved, in line with Gendron and Bendrand's suggestion to note "the significance of actors reflectivity in constituting social realities" (Bédard & Gendron, 2010).

When it comes to qualitative research, Langley distinguishes between those researchers who are formulating "a priori process theories and testing them using coarse-grained longitudinal time series and event-history methods", and those who "plunge into the processes themselves, collecting fine-grained qualitative data […] and attempting to extract theory from the ground up" (Langley, 1999). This thesis is

based on the latter attitude towards collecting qualitative ground-up data with mixed qualitative research (Flick, 2014), using several methods: Analysis of Regulatory and Practitioner Documents (Bauer & Gaskell, 2000), Immersion in the Field (Delamont, 2004; DeWalt & DeWalt, 2010; Jorgensen, 1989; Kawulich, 2005) and Semi-Structured (Gillham, 2005) interviews.

The research aims to illuminate practice, and analyse the micro-practices that work together to provide organisational risk oversight. In order to answer the research questions: 'How does the practice of risk oversight differ from management?', 'How do various actors operationalise their risk oversight roles?' and 'How do information flows shape oversight?', data has been collected from three categories of qualitative sources: (1) documents, (2) field immersions, and (3) interviews. To my knowledge a comprehensive study of this kind has not been done before, due to the depth of data collected from a number of difficult-to-access qualitative sources. Documents were used to trace the evolution of concepts, interviews to understand how practitioners make sense of their roles, and field immersions to see how information flows happen. Chapter 4 is based on content analysis of regulatory documents produced by the Financial Services Authority – the main UK financial institutions regulator in the relevant period. Chapter 5 relies on a combination of interview materials and publications by regulators and consultants. Chapter 6 builds primarily on document analysis, while Chapter 7 is more rooted in the interviews. The two field immersions within firms as well as attendance at many academic and practitioner conferences are primarily used in support of interview and documentary material.

The aim was to develop knowledge of discourse and of how practitioners make sense of their role in the risk oversight processes. The first field immersion was largely exploratory about the current field of risk management in practice, and full time exposure to it in a setting of a financial institution allowed me to be deeply immersed into the topic, instead of formulating beforehand a hypothesis to be tested, the immersion followed the Barker et al view that "an unstructured approach […] is suitable to an under-researched area, because in contrast to a narrower approach of formulating and testing hypotheses, it enables the emergence of

hypotheses that might not have been apparent in advance" (Barker, Hendry, Roberts, & Sanderson, 2012). This lack of a hypothesis is partially creditable for the emergence of the object of analysis: 'risk oversight' as the narrow space for further research, as shown below. While the second participant observation and the interviews were more focused on different aspects of risk oversight, they were not conducted to test hypotheses. The rest of this chapter explains the process of data collection and analysis in more detail.

3.2. Document Analysis

Some argue that content analysis is "the most important research technique in social sciences. It seeks to analyse data within a specific context in view of the meaning someone – a group or a culture – attributes to them" (Krippendorff, 1989). Borrowing from communications research studies, content analysis can be used for many purposes that were classified e.g. by Berelson 1952, including describing trends in communication content and revealing the focus of institutional attention (Berelson, 1952). Document analysis conducted as a part of this research was more interpretative and discursive than pure content analysis, but the choice of the method was informed by the literature on content analysis.

Document analysis informs Chapter 4 (The Emergence of Responsible Oversight), focusing on the evolution of the concept of risk within UK regulation, and Chapter 6 (Risk Oversight in Management), discussing the operationalisation of the 'Three Lines of Defence' corporate governance framework. Content analysis did not include thematic analysis or production of "thematic networks: web-like illustrations (networks) that summarize the main themes constituting a piece of text" (Attride-Stirling, 2001). The reason for that was a methodological decision not to take a narrow evidence sample and investigate micro-patterns within documents, but instead to focus on evolution of key concepts over time.

Due to the choice of the financial industry as a focus of my study, content analysis has been conducted of each publicly available on their website document produced by the Financial Services Authority (and later Prudential Regulation Authority and Financial Reporting Council), and also selectively looked at the documents produced by other regulatory bodies and consulting firms.

In order to analyse all publicly available regulatory documents since the foundation of the Financial Services Authority, the data base on their website was thoroughly investigated, and every single document was searched for key words 'risk' and 'oversight', with a specific focus on the conjunction 'risk oversight', and read the context within which each those terms appeared, as well as copied these paragraphs into a separate timeline. This process allowed observing changes in the regulatory attitudes and opinions about risk oversight. A disadvantage of that approach is that there is a danger of not picking up content when synonyms are used instead of the chosen search words, but the volume of the documents dictated that approach.

Coding of findings, or in other words looking for patterns and common themes, was conducted iteratively as the research went on, in a grounded theory fashion: grounded theory recommends analysis from the onset of the study on because "it directs the next interviews and observations" (Corbin & Strauss, 1990). The reason for that choice in terms of document content analysis was that a chronological timeline was followed, and therefore whenever one of the key terms emerged a description of the context in which it was used was noted. Manual process was used instead of textual analysis software, highlighting the key words within paragraphs that were useful in understanding the regulatory approach to risk and risk oversight. Despite the systematic nature of the identification process of the key themes, it is necessarily limiting due to the fact my personal view of finding significance went into this process, in line with the grounded theory approach.

Chapter 6, which also relies on document analysis, provides an overview of the current understanding of the Three Lines of Defence model. When deciding how to approach this part of research, Stempel's (1952) finding that a small sample, systematically selected, is better than a large sample of materials collected

conveniently (Stempel, 1952) was implemented. Due to an overwhelming supply of available information about it, the sample was limited to the documents produced by selected leading consultancy and professional bodies as examples of thinking, with an attempt to select those who are likely to be most influential.

The purpose of the selected documents was to demonstrate the way practitioners represent their understandings about how the framework is intended to be operationalised in practice. The institutions to focus on were chosen based on their potential perceived impact on the firms under investigation. The assumption made was that the major consultancies would have more impact and should therefore be given more attention in my research.

Specifically, consideration is given to the output of the three major strategy consultants – McKinsey, BCG and Bain, and the Big 4 auditing firms: PwC, KPMG, EY, and Deloitte. Among the professional bodies, the publications of the Institute of Risk Management (IRM), the Institute of International Finance (IIF), and the Chartered Institute of Internal Auditors (IIA) are also examined. While there are clear methodological drawbacks to not using a wider array of institutions, the focus on financial services regulation is justifiable by the fact that the institutions observed and the interviews conducted were all in the financial sector.

Although there is an abundance of publicly available regulatory and practitioner documents, field immersions via internships and interviews are instrumental in order to investigate the way risk oversight and information flows function and are conceptualised in practice. More specifically, field immersions allow light to be shed on these aspects of practice at a level of granularity that is just not possible to achieve through publicly available documents. They also improve the quality of interviews. Power et al (2013) warn that "it is part of the culture of financial services that it is typically difficult to access for external researchers" (Power et al., 2013). The next section expands on the two field immersions, followed by the description of interviews.

3.3. FIELD IMMERSIONS

The practice of risk oversight could be superficially addressed by looking at the macro-level of an organisation through its corporate charts and structures (that are part of sense-making), but this research focuses on the operationalisation of oversight at the level of practice by the actors. This gives rise to the need to observe the practice of oversight at the level of individuals.

In order to avoid the criticism that "Because they are at arm's length from actual practice, [researchers] often fail to reflect the way business works in real life" (Bennis & O'Toole, 2005), following e.g. Mikes (2009), access to two organisations was secured, involving two extended periods in the field exploring those organisations in depth. These observations enabled immersion in the field with the aim of understanding how risk is operationalised within these two financial institutions in practice, as well as gaining trust of and access to interviewees. Spradley explains that "Participation allows you to experience activities directly" (Spradley, 1980), and Stake says that observations are useful because of "revealing actual experience" (Stake, 2013), but warns that the results of observations within one firm are not broadly generalisable, which is a significant limitation necessary in the grounded theory approach to research.

Keeping these advantages and limitations in mind, two extended observations (8 and 9 week-long) were carried out in two major financial institutions: an investment bank in 2012 and an insurance firm in 2013. Both of these immersions into practice were obtained through informal methods, i.e. contacting people within the firms and enquiring whether it would be possible to work for them while also observing the way they work and conducting interviews. The lines of my research project were explained to them in advance. The firms concerned were content to grant access on this basis, and expressed interest in the resulting observations and findings. They imposed no conditions or controls on access of observations, except an expected and understandable requirement for confidentiality.

The immersion in the field had aspects of participant observations, but primarily used to build confidence in the rest of the research and discover interesting aspects to focus on as well as improve the quality of interview findings. During both immersion periods, all the necessary pre-employment checks, compliance training, and then job-related tasks that one would expect from a regular intern were carried out. Some ethnographic theorists warn that the researcher might be seen as an outsider (Bartunek & Louis, 1996) and face difficulties of access once on site (Walsh, 1998), but that has not proven to be the case in my experience, possibly because of my close involvement in the work process.

3.3.1. First (Exploratory) Field Immersion

The first immersion consisted of an eight-week work engagement that was conducted in August and September 2012 in the risk management function at one of the world's top 5 investment banks, employing over 50,000 people globally, and holding over $700 billion in assets. The Risk Management function in that organisation (which is also quite representative of other risk management functions across the financial industry), was split into three silos of Market, Credit, and Operational Risk.

I worked within the risk management division at the head office of the firm's Europe, Middle East and Africa (EMEA) branch as a risk management analyst in the 'Portfolio Analysis' division. The Portfolio Analysis group was created several months before my work there, and positioned above the three silos of risk organisation - it was tasked with information consolidation and processing for use of the top management and the board.

I reported into the Managing Director of the "Portfolio Analysis" group, who reported directly to the EMEA CRO, who in turn reported to the global CRO based in New York. My responsibilities included carrying out quantitative analysis of value at risk[8] (VaR) measurements using Excel and similar internal firm tools and databases. The role included analysing the bank's market position by discovering reasons for the deviations from what might have been expected in light of historical data as well as coming up with forecasts after using complex modelling techniques related to value at risk (VAR). I presented the output of my analysis to my manager via emails, Word reports and PowerPoint presentations that went into the board management information packs for both the EMEA and Global level. I was directly involved in the process of creation of the group's statements and reports that gave me a thorough high-level overview of a risk function within a bank.

The first field immersion was crucial to this research in order to explore the risk management field in practice and formulate the direction of consequent research. The findings from this participant observation triggered my interest in "risk oversight" as a phenomenon, because even though they themselves did not use that term, with an analytical distance I observed that the function I worked for, the "Portfolio Analysis" group was designed to facilitate risk oversight between the three silos of risk and the top management and the board above them by providing them with an overview of the business' risk management profile, which has not been done as methodically prior to the introduction of this function.

---

[8] Definition of VAR: "For a given time horizon *t* and confidence level *p,* the value at risk is the loss in market value over the time horizon *t* that is exceeded with probability 1-*p.* Many firms use an overnight value at risk measure for internal purposes, as opposed to the two-week standard that is commonly requested for disclosure to regulators, and the 99-percent confidence level is far from uniformly adopted." (Duffie & Pan, 1997)

3.3.2. Second (Oversight) Field Immersion

The second period of observations, conducted a year later, was more focused on observing manifestations and actors involved in risk oversight and management information production. It consisted of a 9-week project within a risk management function at a major global insurance firm in August, September and October 2013. The firm has over 24 million customers and £500 billion of assets under management. The risk management function in that firm included a separate "Risk Oversight" group, and I was able to interview all the employees working in that group among other people across the risk management department.

My role there was more of an 'expert' and as such I reported directly to the Global Chief Risk Officer and his two vice-heads. I worked on a number of projects for each of them, which provided me with broad exposure to high-level strategic decisions, although as a trade-off it came at the price of making it harder to observe the micro-level interactions between the risk managers who were working in lower roles within the department. The reports were much more qualitative than those in the first institution - I did not conduct any Value at Risk calculations, and my work was focused on the corporate governance of the risk department and their management information flows.

As the goal of both participant observations was to describe the practice of risk management and oversight without "imposing a priori a specific theoretical lens" (Anderson & Widener, 2006), I was observing as much as I could and attended as many meetings as was possible during the time I had, which was necessarily limited as this was carried alongside doing my actual job at the company.

The main challenge I experienced when it came to the choice of participant observation as a research method in both cases was described by Delamont: "Ethnography is hard work: physically, emotionally and mentally exhausting" (Delamont, 2004), and indeed I found it very challenging to multitask between the

two roles: having both to work full-time for these firms, performing the tasks of a regular employee, and keeping some distance while observing them in my academic capacity.

The findings of this thesis are therefore not strictly ethnographic, because the primary purpose of the field immersions and observations was two-fold: to gain access to people I have interviewed and to provide background knowledge from the field in order to make interpretations about interview material and give deeper sense of practice. In addition to this, participant observations were intended as a means to improve the quality of the interviews since by the time I conducted interviews within the firms I had already established rapport with the interviewees, having worked together with them for several weeks – and one of the key advantages of participant observation is that it enables "researchers to know what questions to ask" (Bernard, 2011). It has also improved the interviews I conducted in other institutions because of my deeper understanding of the field.

3.4. INTERVIEWS

During both observation periods, I met many people across different departments within the risk management, internal audit and regulatory compliance divisions, and I held both informal, so-called "water-cooler" interviews as well as others more formal in nature that were recorded and transcribed. Delamont observed - "Participant observation is used to cover a mixture of observation and interviewing" (Delamont, 2004) – I found it useful to have worked alongside the people I later interviewed because they were very open to speak to me because they already knew me by that point. I found, however, that interviews outside of the organisations I observed were also enhanced by my prior immersion in the industry, even without the benefit of knowing these people or their organisations first. Most quotes used in the thesis stem from formal, recorded interviews, but some of the questions were inspired by the topics that arose during the less formal interactions.

These less formal interactions and observations also fed into increased knowledge of the field and resulted in my ability to ask better questions.

In addition to an immense number of informal conversations with practitioners both during my participant observations and at the outside events and conferences, I conducted 67 semi-structured interviews: each interview lasting between 25 and 97 minutes, 60 of them were transcribed and recorded, detailed notes were taken during the remaining 6 interviews. Interviewees included those working in risk management divisions in at the two firms where the participant observations were held as well as staff from other major financial institutions. In terms of the hierarchical levels, interviewees included: several CROs of largest banks and insurance firms, Managing and Executive Directors, Vice Presidents, Associates and Analysts, which gave me a clear view of the full spectrum of risk management and regulation across various levels of seniority and experience within the industry.

The transcribed and recorded interviews could be divided into three categories: (1) 24 within the financial institution where the first participant observation was conducted and several from other similar institutions, (2) 21 within the insurance firm which was the site the second field immersion, and from similar firms, and (3) 15 Non-executive directors from major financial institutions, including a senior-level regulator and a consultant who work on issues related to NEDs. The goal was not to compare these groups, or insurance and banks, but rather to discover the way risk oversight is operationalised within various financial institutions, without a particularly narrow focus on particular aspects of industries where these interviews were conducted.

The tables below list interviewees within the firms. The first set of interviews – within the investment bank – were quite explorative in nature and included broad questions about their role and interactions with other employees. Those open-ended interviews based on broad themes provided data that was helpful in order to develop further interview design (see Appendix I and II). This method has several advantages, as Sauder and Espeland (2009) agree: “This format provided the flexibility to probe responses, adapt questions to the unique experience and

expertise of informants, pursue emerging insights about processes for which there is, as yet, little systematic empirical evidence, and corroborate suspect information" (Sauder & Espeland, 2009). These interviews provided background knowledge to the functioning of risk management divisions in practice.

TABLE 3.1: LIST OF INTERVIEWEES WITHIN THE INVESTMENT BANK

Code	Position	Firm	Mins
Bank_1	Executive Dir. - Credit Risk: Insurance	Top Investment Bank	27
Bank_2	Executive Dir. - Credit Risk: Commodities	Top Investment Bank	28
Bank_3	Associate Credit Risk	Top Investment Bank	41
Bank_4	Associate Credit Risk Reporting	Top Investment Bank	25
Bank_5	Executive Dir. - Portfolio Analysis	Top Investment Bank	31
Bank_6	Vice President - Market Risk reporting	Top Investment Bank	55
Bank_7	Ex-CRO of top 10 Investment Bank	Top Investment Bank	98
Bank_8	Associate Credit Risk	Top Investment Bank	52
Bank_9	Executive Dir. - Credit Risk	Top Investment Bank	26
Bank_10	Associate - Credit Risk: Commodities	Top Investment Bank	44
Bank_11	Vice President - Credit Risk: Utilities	Top Investment Bank	34
Bank_12	Executive Dir. - Credit Risk: Loans	Top Investment Bank	29
Bank_13	Executive Dir. - Market Risk	Top Investment Bank	36
Bank_14	Vice President - Credit Risk: Europe	Top Investment Bank	32
Bank_15	Vice President - Operational Risk	Top Investment Bank	34
Bank_16	Executive Dir - Credit Risk	Top Investment Bank	33
Bank_17	EMEA risk COO, S&P100	Top Investment Bank	36
Bank_18	EMEA CRO, S&P100	Top Investment Bank	23
Bank_19	Global CRO, S&P100	Top Investment Bank	64
Bank_20	Vice President - Credit Risk: Eastern Europe	Top Investment Bank	25
Bank_21	Associate - Portfolio Analysis	Top Investment Bank	30
Bank_22	Analyst - Operational Risk	Top Investment Bank	20
Bank_23	Head of Group Policy Framework	Top Retail Bank	120
Bank_24	Partner - Big 4 Risk Advisory	Big 4	40

The second category of interviewees was mostly carried out within an insurance firm where the second participant observation was conducted, and other firms of similar size. These interviews were semi-structured and the goal was to discover attitudes to and understandings of the Three Lines of Defence corporate governance framework (which was discovered when investigating risk oversight within the firms – more information on that in Chapter 6), about interaction between the lines and Information Flows: findings from these interviews are primarily discussed in Chapters 6 and 7.

TABLE 3.2: LIST OF INTERVIEWEES WITHIN THE INSURANCE FIRM

Code	Position	Firm	Mins
Insurance_1	Head of Capital Management	Top Insurance firm	48
Insurance_2	Internal Audit Director	Top Insurance firm	40
Insurance_3	Audit	Top Insurance firm	33
Insurance_4	Analyst in ERM group	Top Insurance firm	47
Insurance_5	Head of Insurance Risk and Model Oversight	Top Insurance firm	74
Insurance_6	Head of ERM	Top Insurance firm	41
Insurance_7	ERM team	Top Insurance firm	25
Insurance_8	Variable Annuities	Top Insurance firm	48
Insurance_9	Head of Risk Oversight	Top Insurance firm	26
Insurance_10	Head of Internal Audit Finance	Top Insurance firm	37
Insurance_11	Manager of Capital Management	Top Insurance firm	35
Insurance_12	Ex-CRO, head of Investment	Top Insurance firm	21
Insurance_13	Vice-CRO	Top Insurance firm	25
Insurance_14	Head of Risk: Model side	Top Insurance firm	47
Insurance_15	Head of Internal Audit	Top Insurance firm	42
Insurance_16	Head of Risk Oversight	Top Insurance firm	64
Insurance_17	Head of Market Risk	Top Insurance firm	43
Insurance_18	CRO	Top Insurance firm	34
Insurance_19	VP Model Validation	Top Insurance firm	63
Insurance_20	Capital modelling team lead	Top Insurance firm	34
Insurance_21	Chairman of a major insurance firm	Top Insurance firm	130

To complete the discussion of risk oversight, 15 interviews were conducted with the risk committee chairmen and board members of some of the largest financial institutions, primarily based in London, each of them lasting 47 minutes on average. Only one of these interviewees was on the boards of the institutions in which the field immersions were carried out. One CRO, strategy consultant, and regulator are included in this list due to the nature of topics discussed with them.

TABLE 3.3: LIST OF NED INTERVIEWEES

Code	Position	Firm	Mins
Interviewee_1	Chair Risk Committee	Top 10 Bank	23
Interviewee_2	Chair Audit Committee	FTSE100 Insurance	42
Interviewee_3	Ex-CRO, Risk Co member	FTSE200 Insurance	55
Interviewee_4	Chairman	Top 10 Insurance	51
Interviewee_5	Chair Risk Committee	FTSE100 Insurance	46
Interviewee_6	Chair Risk Committee	Top 10 Insurance	36
Interviewee_7	CRO	FTSE100 Bank	67
Interviewee_8	Chair Risk Committee	European Retail Bank	55
Interviewee_9	Chair Risk Committee	FTSE100 Bank	45
Interviewee_10	Chair Risk Committee	Top 10 UK Bank	34
Interviewee_11	Member Risk Committee	Top 10 Bank	49
Interviewee_12	Chair Risk Committee	Top 10 Bank	53
Interviewee_13	Member Risk Committee	Top 10 Bank	34
Interviewee_14	Partner	Consultancy	32
Interviewee_15	Ex-Chairman	UK Regulator	26

These interviews were conducted in batches: the first in August-September 2012, during the first field immersion in an investment bank and shortly thereafter, the second during the second field immersion in September-October 2013, and final in May-June 2014 (penultimate year of this research project). The average length of

an interview within the first cohort was 41 minutes (37 minutes within the investment bank where the first field immersion was conducted, 34 minutes adjusted for the outlier longest interview). Within an insurance firm, the average length of an interview was 45 minutes (41 excluding the outlier).

There are two factors that might explain why the interviews were on average 8 minutes shorter within the investment bank than the insurance firm: firstly, these interviews were more exploratory in nature - I was less experienced and had a less clear interview protocol. Secondly, the investment bank interviews were conducted within the scope of the "coffee-breaks" that were socially accepted within the bank, and typically lasted for about half an hour. Within the insurance firm, I had more watercooler and lunchtime conversations beforehand, which resulted in interview material being more rich and more directly quoted in the remainder of this thesis.

The average interview with a NED lasted for 43 minutes, which is more than I expected when I started these interviews, because I was aware of seniority and busy schedules of these people. NED interviews were quite rich, possibly due to the fact that by the time that I conducted these interviews in the summer of 2014, I was able to contribute to the conversation in a way that these interviewees also found useful. While the number of NED interviews is lower than other categories of interviewees, it is crucial to emphasise the seniority of these people: being so senior allowed them to have a long experience as overseers and thus be able to answer in-depth questions about their sense-making of 'performing oversight'. Additionally, these people are major actors who contribute to the public discourse about their role in risk oversight (through their interactions with regulators, participation in conferences for NEDs, and publications), and can therefore be seen as opinion formers. It was possible access these people though a personal network and later also a snowballing effect: indeed, all but one NEDs who were approached agreed to be interviewed and recorded.

Most of them are NEDs in the FTSE100 firms, primarily from the largest financial institutions which are frequently discussed in the media and regulatory documents, thus they bring quite a unique perspective to research. Furthermore, most of those people have told me they have never been interviewed in an academic

setting before. Eisenhardt and Graebner say the best way to mitigate the possible data bias in interviews "is using numerous and highly knowledgeable informants who view the focal phenomena from diverse perspectives" (Eisenhardt & Graebner, 2007), and the seniority as well as the fact that my interviewees come from different institutions all help to do that.

The findings presented in Chapter 5 come from the NED interview material, based on the individual's perceptions of his or her role. However, these findings are qualified by an inherent weakness of the interview methodology: since this research is based on what could be described as actors' representations of themselves – the unit of analysis is their own representations about their jobs, not facts. I treat interviews as a constructed image that people portray of themselves, and therefore as a fact of their reality and implicitly, as I assume that what they tell me is trustworthy, everything they tell me about themselves does indeed become a fact in a performative manner.

During the interview analysis process, I treated people's descriptions of their actions as being analogous to their actions, and participant observation findings are complementary to the interviewees' descriptions. I do not consider interviews from an overly sceptical perspective, and do not assume that interviewees framed their responses based on their "assumptions of what the researcher is up to" (Alvesson, 2003). Indeed, as all interviewees were assured full anonymity, it is assumed here that their responses are fully representative of what they truly think they do.

My goal was not to find "how it is really done", or some other ultimate "truth" about the organisational reality, but rather to demonstrate examples of perceived practice and their implications for future research. It is relevant to note that in most cases the interviewees were answering questions of this kind for the first time, which in research terms is close to a 'greenfield site'.

Furthermore, when discussing what the Non-executive directors do, I am not attempting to determine what they should be doing (which is informed by the corporate governance codes and legal precedents), but rather what they are actually

doing, or more precisely what they think they are doing. The full interview protocol of these semi-structured interviews which I conducted can be found in Appendix 1.

These questions were chosen in order to understand the NEDs' perceptions about the nature of their role in a relatively open-ended but directed way and they naturally pre-determined the themes that will be discussed in Chapter 5, such as NEDs' representations about their role, including the discussion of the meaning of their oversight role, and also their definitions of success and failure. Additionally, as a part of these definitions of success and failure, conversations often included discussions on independence and the length of terms of office.

In line with the LSE research ethics guide (LSE, 2015), I informed each interviewee about complete confidentiality and anonymity. I also asked for their consent to use what they say in line with the Chatham House rule, namely: "participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed" (RIIF, 1927). Using the Chatham House rule is the reason this thesis does not mention their names or institutions, nor the names of people or institutions they mentioned during the interviews. Following this rule also allowed me, during the debriefing part of the interviews, to share what I discovered from other interviewees – that in turn made the interview useful for the interviewee and made it easier to contact them again for clarifications or additional information.

I transcribed several hours of interviews myself, but most other interviews were transcribed by professional transcription services. When analysing the themes occurring, I chose not to use nVivo or other interview coding software because while there are certain advantages to formal approaches, I decided that opting for reading paper print-outs of interview transcripts and highlighting them with different colours and notes was a more convenient method that allowed me to be more immersed into data, and coding it on the computer after the rounds of highlighting and annotations on paper seemed redundant.

3.5. IDENTIFYING THEMES

When It comes to data analysis, I followed the approach outlined by Dent (1991) during his study of organisational cultures, which involved "arranging the different types of data chronologically and identifying common themes and unique insights" (Dent, 1991). Due to the continuously developing nature of the themes I was investigating, analysis was done in a continuous chronological manner with additional data points investigated as they were added.

The research focus here is on the actors' sense-making, therefore "data tend to be eclectic, drawing in phenomena such as changing relationships, thoughts, feelings, and interpretations" (Langley, 1999), and grounded theory approach to identifying themes was chosen as the most appropriately fitting one. When it comes to qualitative research, "It can be argued that reliability is an impossible criterion to achieve in practice as different researchers will always produce different versions of the social world" (Bloor & Wood, 2006). While it is inevitable in semi-structured interviews and field observations, when it comes to document analysis I have given a lot of thought to the appropriate selection of the documents to review (e.g. every FSA document was looked at) in order to make the findings as reliable as possible. The document content analysis sections of this thesis are particularly replicable if the above-mentioned methodology was to be followed, as all the documents used are available in the public domain.

The chronological approach to collecting data in real organisational setting as well as looking at regulatory and consultancy documents continuously as they were published has many advantages in terms of relevance and timeliness, but also presents a number challenges. One of the difficulties identified by Langley regarding collecting data in the organisational context is "they often involve multiple levels and units of analysis whose boundaries are ambiguous" (Langley, 1999).

I departed from the grounded theory approach in that iteratively with developing the findings based on practice observations, interviews, and document reviews; I used pre-existing theories outlined in the previous sections as tools with explanatory value of the concepts discussed. The choice of these theories was necessarily subjective, but I rooted most empirical exploration of concepts in agency and regulation theories as the two widely used and accepted theories in accounting and management research. The following chapter presents an overview of the historic emergence of oversight that provides the background to the remainder of the thesis.

CHAPTER 4: THE EMERGENCE OF RESPONSIBLE OVERSIGHT

4.1. INTRODUCTION

In the aftermath of the global financial crisis, regulators were frequently blamed (Davies, 2010) for their lack of involvement in the business practices that would allow them to prevent firms from misbehaving. These failures were highlighted in the UK in the Walker Review of Corporate Governance published in November 2009. That report also led to an increased focus by the UK regulators on the work of risk managers and of boards. Since then regulators have further increased their focus on firm-level oversight activities, where oversight is seen as a solution-language to the problems that were illuminated during the financial crisis. The practice of risk oversight in financial firms is heavily and increasingly influenced by the views and policies of financial regulators.

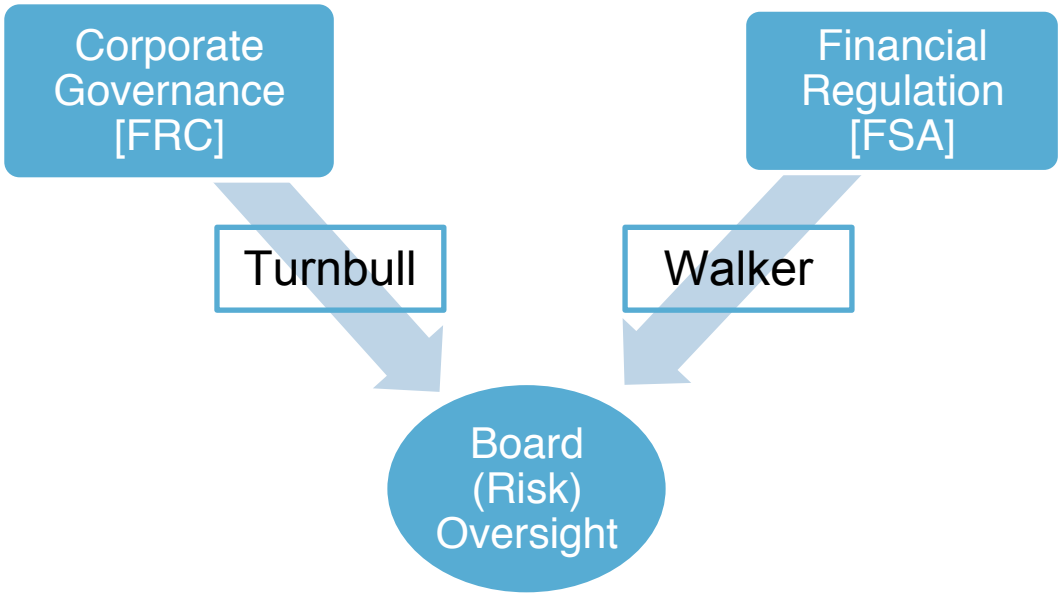
This chapter investigates *how* has the regulatory attitude to risk oversight evolved before and after the global financial crisis, and how does regulatory attention regarding oversight manifest itself. The prime focus here is on the changing views of regulators in the UK, as they have directly influenced the behaviours of financial firms in London, where my research is focused. Some international references are provided for context, but this chapter does not attempt to conduct a comprehensive review of the international financial regulation landscape, which would be an unmanageable task within the constraints of this research.

In order to provide a background to the rest of this thesis, this chapter gives a document-based chronological overview of the UK regulatory statements regarding corporate governance generally and financial regulation more specifically, and tracks the way the Financial Services Authority's discourse about risk changed over time. The Financial Services Authority (FSA) was the main financial regulator in the UK up to April 2013, and has been split into Prudential Regulation Authority and Financial Conduct Authority since. To demonstrate the evolution of the FSA's ideas about the regulation of risk, I started at its foundation time, looked at every single publicly available document FSA produced, and read all the references to 'risk' and 'oversight', as was discussed in more details in the Methods chapter. This chapter shows the shift of regulatory focus towards the creation of 'responsibilised risk overseers', and the tools such as risk appetite and risk culture that these overseers are expected to use.

The chapter is organised the following way: firstly, the evolution of corporate governance regulation in the UK is investigated in a timeline manner. Then attitudes to risk in financial regulation are examined and the finding is that while they started off as two independent strands of regulatory space, over time they converged into both being interested in board-level risk oversight. This therefore leads into the next Chapter which is about boards.

Figure 4.1 presents a topological summary of the way regulation has gravitated towards focusing on firm-level governance and boards. Financial Reporting Council (FRC) focuses on corporate governance for all firms, and Financial Services Authority (FSA) specialises on the financial regulation, but over time both of them became interested in risk governance – the remainder of the chapter traces that evolution .

FIGURE 4.1: REGULATORY CONVERGENCE



While these two regulatory strands used to be focused on different areas, over time they both became similarly interested in the firm-level risk oversight. The two points identified where that became particularly visible are the 1999 Turnbull report "Internal Control: Guidance for the Directors on the Combined Code" and the 2009 Walker review "of corporate governance in UK banks and other financial industry entities". Although Turnbull triggered the importance of explicit Board involvement in the internal control matters through reinforcing earlier documents suggesting a variation of aspects of it, Walker is a point where board-level risk oversight particularly expanded in financial firms.

Walker also acknowledged potential overlaps between his suggestions and the Financial Reporting Council's update of the Combined Code on Corporate Governance: "Simultaneously with this Review, the Financial Reporting Council

(FRC) is undertaking a consultation on the Combined Code on Corporate Governance (Combined Code) for all listed companies and, given the clear potential overlap, Sir Christopher Hogg (as chairman of the FRC) and I have co-operated closely throughout. Implementation of some of these will require specific initiative by the FRC or the FSA" (Walker, 2009).

Table 4.1 presents a timeline overview of the corporate governance and financial regulation documents that will be mentioned in the remainder of this chapter.

TABLE 4.1: DOCUMENTS TIMELINE

Date	**Reports**
Dec 1992	Cadbury Report "Financial Aspects of Corporate Governance", on corporate governance generally.
Dec 1994	The Rutteman Report: "Internal control and financial reporting - guidance for directors of listed companies registered in the UK"
Jul 1995	Greenbury Report on Directors' Remuneration,
Jan 1998	Hampel Report "Review of corporate governance since Cadbury"
Jun 1998	Hampel Combined Code on Corporate Governance
Sep 1999	Turnbull Report "Internal Control: Guidance for Directors on the Combined Code"
Jan 2003	Higgs Report "Independent review of non-executive directors".
Jan 2003	Smith Report "Audit Committees: Combined Code Guidance"
Jan 2003	Tyson Report on the Recruitment and Development of Non-Executive Directors
Jul 2003	The Combined Code on Corporate Governance
Oct 2005	"Internal Control: Guidance for Directors on the Combined Code" (revised Turnbull)
Jun 2006	The Combined Code on Corporate Governance: update
Jun 2008	The Combined Code on Corporate Governance: update
Oct 2008	FRC Guidance on Audit Committees (revised Smith)
Nov 2009	Walker Review (2009) "A review of corporate governance in UK banks and other financial industry entities" in response to the financial crisis
May 2010	The UK Corporate Governance Code: update of the Combined Code on Corporate Governance
Dec 2010	FRC Guidance on Audit Committees: update
Feb 2011	Lord Davies Review: Women on Boards
Mar 2011	FRC guidance on Board effectiveness
Sep 2012	FRC Guidance on Audit Committees (revised 2008 and 2011 guidance)
Sep 2012	FRC Corporate Governance Code
Jun 2014	PRA: "PRA's approach to Banking Supervision"

Sep 2014	FRC Risk Guidance: "Guidance on risk management, internal control and financial and business reporting"
Sep 2014	FRC Corporate Governance Code
May 2015	PRA "Corporate governance: Board responsibilities" Consultation paper
Jul 2015	PRA "Strengthening individual accountability in banking"

Source: Own summary from FRC, FSA, PRA, and FCA data bases.

4.2. CORPORATE GOVERNANCE IN THE UK

4.2.1. BACKGROUND

One of the foundational documents for the current corporate governance frameworks is the 1992 Cadbury Report: "Financial Aspects of Corporate Governance", which was published in December 1992 in response to a series of financial scandals, including the Maxwell case. The failure of Maxwell Communications, following a series of acquisitions, partly financed by the diversion of funds from employees' pension funds, highlighted the weakness of the group's governance. Other failures, such as the collapse of the fraudulent bank BCCI, and of Polly Peck, a rapidly expanding textile company, drew further attention to the failures of boards to oversee company decision-making. These problems stimulated the establishment of the Cadbury Committee to review British corporate governance and propose improvements[9].

The Cadbury report was "explicitly designed to improve internal control mechanisms, based on the assumption of a relationship between internal control, financial reporting quality and corporate governance" (Spira & Page, 2003). The

[9] For more information about these cases see "In Letter but not in Spirit: An Analysis of Corporate Governance in the UK" (Arcot & Bruno, 2006)

review “adopted the view that directors’ responsibilities with regard to internal control should be clarified” (Spira & Page, 2010) with the intention to "strengthen trust in the corporate system” (Cadbury, 1992).

Specifically, Cadbury’s main recommendations were to (1) separate the roles of the CEO and the Chairman of the board (which has been influential in the UK and Europe, but is still not normally the case in the US), (2) introduce “a minimum of three non-executive directors”, which is needed in order to fulfil the “recommendations on the composition of sub-committees of the board” (Cadbury, 1992), and finally (3) introduce Audit Committees in all listed companies. At the time, according to the report, two-thirds of the top 250 UK listed companies already had them in place, influenced by the fact that since 1978 the presence of the independent audit committee had been a requirement for all companies listed on the New York Stock Exchange.

By introducing these three fundamental requirements, the Cadbury Report began the process of greater codification of corporate governance norms in the UK which apply to all listed companies. “In effect the 1992 Cadbury Report was a policy initiative which legitimated the widening of enterprise control practices to encompass risk management and corporate governance issues” (Bhimani, 2009), a development that has been continuous since.

Since 1992, the UK has been implementing developments of Cadbury’s recommendations at regular intervals and has progressively introduced a system of both hard and soft law to strengthen its corporate governance framework. For example, in July 1995 the Greenbury report (Greenbury, 1995) on the remuneration of directors was published by the Confederation of British Industry. This report followed the public anger over executive pay, specifically the case of British Gas, when the chief executive’s 75% pay increase in 1994 sparked what was known as the 'fat cat' controversy. The Greenbury report introduced the requirement for a remuneration committee of the Board and also encouraged changes in pay to incentivise long-term behaviour.

The Hampel Report (Hampel, 1998) followed in January 1998. It clarified and combined recommendations of the Cadbury and Greenbury reports, and later became known as the "Combined Code". One of the key messages of the "Combined Code" was that: "Companies should be ready to explain their governance policies, including any circumstances justifying departure from best practice", (Hampel, 1998), which introduced the UK's "comply or explain" regulatory approach based on principles rather than rules. This approach "has been widely admired and imitated internationally" (FRC, 2014b).

Following the 1998 "Combined Code", the Turnbull "Internal Control: Guidance for Directors on the Combined Code" was published in 1999 (and updated in 2005). The main contribution of the Turnbull report was that it made the "Combined Code" more practical and understandable to firms and provided implementation guidance on internal controls reporting. It gave a detailed overview of the directors' responsibilities for best practice regarding internal controls and risk management, and explained that boards need to continuously review and approve them. Indeed, some critics explained that the Turnbull report "epitomised" the convergence of thinking about "corporate governance, risk management, and regulation" (Hutter & Power, 2000), and idealised the idea of a "top-down, integrated risk management policy".

Additionally, according to Power,

> "Combined Code on corporate governance represents a new style of regulating the organisation. For such a style to succeed, the inside of organisations and their internal control systems must be reconceptualised as a potential 'regulatory space'. However, the point is not to control the corporation with more regulation from the outside, but to encourage the development of a transparent inner space for self-regulatory capacity" (Power, 2000).

This observation contributes to explaining the way increased self-regulation lead to the creation of boards as internal control 'pseudo-regulators'.

The Higgs review (Higgs, 2003): "Review of the role and effectiveness of non-executive directors", recommended several improvements to the Combined Code, and directed the focus of the Code towards "behaviours and relationships and

the need for the best people, which are essential for an effective board". The report was produced as a response to the ENRON and WorldCom scandals in the US, and while still supporting the "comply or explain" approach to regulation, it also outlined a number of provisions that made the requirements regarding board composition stricter. For example, it suggested that at least a half of the board has to be made up of independent NEDs, introduced annual evaluations of the directors' performance and the concept of term limits. After nine years of service a board member may be deemed no longer independent.

All these corporate governance codes apply to UK listed companies generally. A further set of requirements had been imposed specifically on regulated firms in the financial sector. The next section discusses these financial regulation requirements.

4.2.2. FINANCIAL REGULATION: FINANCIAL SERVICES AUTHORITY

The Financial Services Authority (FSA) was the main UK financial regulator from June 1997, when "responsibility for banking supervision was transferred to the FSA from the Bank of England" (FSA, 1997b) up to April 2013. FSA was founded as the combination of nine earlier regulators, and was sometimes nick-named "The City's super-watchdog" (BBC, 2001) because of its wide mandate. "As they merged, it was apparent that not only did their practices and culture differ, they also had a completely different language for describing risk, and indeed that there was no commonly understood meaning of the terms 'regulation', 'supervision' or 'enforcement'" (Black, 2004). Due to the diversity of these previous bodies, it was important to create a universal framework which would make the FSA a coherent organisation with clear objectives and clear ways of achieving these objectives.

From the very beginning of its existence, the FSA declared its commitment to a 'risk based approach' to regulation and supervision as the first point in the "style and process of regulation" section (FSA, 1997a) of the first document they

produced. The FSA's risk-based approach provided a solution in that it, according to the analysis of its objectives, was intended to "concentrate regulatory attention where problems are most likely to occur, and would focus on themes rather than structures" (Economist, 2000). When the FSA spoke about this approach to regulation during these initial stages, it did not intend "risk" to be interpreted as risk within the firms themselves, but rather risk to the objectives of the financial regulator (Black, 2004).

In 1998, soon after its foundation, the FSA formulated the RATE (Risk Assessment, Tools, and Evaluation) framework. The FSA inherited the RATE framework from the Bank of England where it has been under development since 1996. Within the Bank of England, RATE evolved under the supervision of deputy governor Howard Davies (Black, 2004) who became the first chairman of the FSA in 1997. "The Bank of England approach emphasized the common interests of management and supervisor. The intensity of external supervision and of audit could be varied depending on the control culture in the target bank" (Power, 2007) This approach of focusing on common interests of management and supervisor transferred from the Bank of England into the FSA's approach to RATE.

The Risk Assessment, Tools, and Evaluation (RATE) framework was discussed (FSA, 1998) as the introductory model of the FSA's approach to regulation. "In developing RATE, a significant driver was the need to defend itself against critics of its supervisory abilities" (Black, 2004), which is alluding to the fact that at that stage the FSA was only interested in risk within firms if this risk endangered its objectives as a regulator.

As a part of implementing the RATE framework, the FSA conducted on-site assessment visits to the firms it was supervising in order to "improve the FSA's understanding of the business and control risks run by the bank" (FSA, 1998). During this period, the FSA became more explicit about its own "oversight" role and how it would assess and monitor risks within the businesses. The fact that the FSA spoke about "controlling" risks run by the bank, instead of just observing or monitoring, is also a new development at that time. The exhibit below demonstrates

a depiction of the RATE model according to the FSA's (1998) "Risk Based Approach to Supervision of Banks" statement.

RATE documents identified three sources of risk: "the external environment, consumer and industry wide developments (CIW) and regulated institutions" (Black, 2004). To demonstrate the originally narrow and regulator-focused attitudes to oversight, it should be observed that the word "oversight" in 1998 and 1999 was only mentioned in the RATE framework documents in the context of regulatory oversight of the firms' actions.

The FSA's four statutory objectives were defined by the 2000 Financial Services and Markets Act (FSMA, 2000) as: market confidence, financial stability, securing the appropriate degree of protection for consumers, and the reduction of financial crime.

The Financial Services and Markets Act 2000 marks an important turning point in government policy towards regulation - in fact, according to my interview with the first chairman of the FSA (Interviewee_15, 2014), regulators before the FSA demonstrated little interest in the risks firms were taking, as long as these were not disruptive for market confidence or apparently harmful for consumers; the regulator's risk appetite encouraged a relatively open approach to risk, with an underlying belief that good risk management within firms would promote regulatory objectives (Baldwin, Hood, Rothstein, Hutter, & Power, 2000). At the same time the Bank of England was given a parallel objective on financial stability, and Treasury responsibility for the overall institutional structure of financial regulation in a Memorandum of Understanding, signed between the FSA, the Bank of England, and the Treasury (Bank of England, FSA, & Treasury, 2000).

In addition to its role in aligning the objectives of nine earlier regulatory bodies that went into the formation of the FSA, RATE also served as a stepping-stone towards ARROW (Advanced risk responsive operating framework). The FSA launched the ARROW regulatory model in 2003, which was aimed at, in their words, making "risk-based regulation operational" (FSA, 2006). Discussing ARROW Power says: "The approach has been internalized and interactions between

FSA and regulated entities are structured by an assessment of the risks they pose to the statutory objectives of the regulator" (Power, 2007). This is important to note, because at this stage of its development, FSA was still primarily interested in risk to its own objectives, not internal risks within the banks, which were still considered to be fully the responsibility of the management and boards of banks themselves, or the macro-prudential risks of interactions between individual banks that became an issue of interest even later.

For example the FSA's 2008/09 Annual report mentions (but does not define) oversight 13 times, but in all cases the focus is on the FSA's role in financial regulation, for example: "We […] have significantly increased the intensity of our oversight of major firms" (FSA, 2008). During this period, the FSA first became more explicit and clear about its own oversight role, identifying the major firms and increasing intensity of oversight over them. The intensification of oversight was also triggered by the fact that the FSA's style of regulation was evolving during that time.

The Turner review "A regulatory response to the global banking crisis" (FSA, 2009b) published in March 2009 "has committed the FSA to more intervention […] significantly less reliance on market discipline, and more intrusive supervision. Although it does not focus directly on principles-based regulation[10] (for more on the theoretical meaning of the principles-based regulation see Chapter 2), the Review is associated with a withdrawal from principles-based regulation" (Baldwin et al., 2010). The Global Financial Crisis was an influential event that set the tone for a lot of the financial regulation since. The following section discusses some of the relevant issues that were brought into light as a result of the crisis.

[10] For more information about FSA's attitudes to principles based regulation, please see – "Principles Based Regulation: Focusing on the outcomes that matter" (FSA, 2007)

4.3. GLOBAL FINANCIAL CRISIS

Prior to the Global Financial Crisis, it was assumed that firms themselves had a powerful incentive to manage their own risks, because if they did not do so they would incur losses and destroy shareholder value. Consistent with that view, the financial regulators in all major financial centres including London took a laissez-faire approach to overseeing the financial sector, often described as a 'light-touch approach' (Alford, 2010). In light of the financial crisis light-touch regulation has been questioned in the UK and elsewhere: Alan Greenspan, former Chairman of the Federal Reserve, said during his testimony in Congress in October 2008 "I made a mistake in presuming that the self-interests of organisations, specifically banks and others, were such as that they were best capable of protecting their own shareholders and their equity in the firms" (Barwell, 2013).

The fact that the banks were not able to manage risks fully could have been caused by: [1] them not understanding these risks well enough, and [2] tension between the profit-generating front office and the risk management function being amplified by the pursuit of short-term profits and [3] incentive structures which encouraged risky behaviour in pursuit of short-term profit (Davies, 2010) – indeed, "the focus on short-term rewards without considering long-term consequences played the critical role in fomenting the crisis as well as being the driving force behind its ultimate severity" (Prager, 2013). Risk Management, where it existed, was not robust enough, or sufficiently strongly supported by top management (Ellul & Yerramilli, 2013), to offset the powerful incentives for personal enrichment through taking risks, especially by taking on additional debt.

Perceived cultural problems, such as short-termism and reckless risk taking behaviour, were retrospectively highlighted as some of the key reasons for the problems that banks faced in the late 2000s. However, these problems did not develop overnight. Specifically, one possible explanation of these "cultural

challenges" the banks are facing could be seen as having "their roots spreading back well over 20 years and can be linked, from a UK perspective, to the 'Big Bang' deregulation of the financial services industry in 1986" (Salz, 2013). This so-called 'Big Bang' de-regulation was triggered by political demands to increase the competitiveness of the City of London as a Global Financial Centre and to break open cartels which were thought to operate against public interest. As the rest of this thesis is looking at primarily investment banks and insurance firms, it is worth noting here that 'Big Bang' essentially affected investment banking and security trading, and did not have a direct effect on retail or commercial banks, or on insurance firms, while the more recent regulatory changes explained later in this chapter have affected all types of firms.

The 'Big Bang' de-regulation reform successfully achieved its aim of making London more competitive, and led to an increase in market activity, which in turn has put London at or the very near the top of the world's financial centre rankings – top in 2013, and second after New York since (ZYen, 2015). Some, however, including Nigel Lawson, who was the Chancellor of the Exchequer at that time, now argue that the global financial crisis of the late 2000s was an "unintended consequence" of the 'Big Bang' (BBC, 2010).

The Financial Crisis has demonstrated that the "self-interests" of the financial institutions themselves were not powerful enough, according to many observers, to reinforce sufficient incentives to self-regulate, and individuals within them were able to circumvent controls on risk-taking in their personal interests. It also appears that financial firms significantly underestimated the risk of extreme market movements, and failed to understand the deepening linkages between firms and markets and the resulting contagion risks.

Despite the apparent failure of firm-level risk oversight during the crisis, there has been an increased demand for more of it – both in the UK and internationally. The Walker review (discussed later) has been particularly influential in shaping the response to the failure of oversight in the UK, but there have also been some international developments affecting major banks in all countries. Regulators have eventually pursued a two-track agenda, strengthening their own direct regulation of

financial firms, on the one hand, and seeking to make internal control mechanisms more robust, on the other.

The Basel Committee for Banking Supervision, the main influential standard-setter in global financial regulation, comprising of current prudential supervisors from member central banks and financial regulators, produced a "Principles for enhancing corporate governance" (BIS, 2010a) consultative document in March 2010, which later resulted in a final document in October 2010 (BIS, 2010b). The report highlighted principles of board governance, risk management, and internal controls. It explained that the board needs to be "supported by competent, robust and independent risk and control functions, for which the board provides effective oversight" (BIS, 2010b). It also suggested that the board's remit includes approval and oversight of "the implementation of the bank's overall risk strategy, including its risk tolerance/appetite" (BIS, 2010b).

The European Commission published an accompanying working document entitled "Corporate Governance in Financial Institutions: Lessons to be drawn from the current financial crisis: best practices" (Commission, 2010) that discusses the significance of the role of the boards in risk oversight and also brings further focus on the non-executive directors as playing a crucial role in the risk oversight process.

The Organisation for Economic Co-operation and Development (OECD) produced their "Corporate Governance and the Financial Crisis"[11] (OECD, 2010) report in February 2010. The report analysed weaknesses of corporate governance in "risk management, board practices and the exercise of shareholder rights" and issued recommendations about these topics.

---

[11] "The basis for this framework is found in the OECD 1999 Principles of Corporate Governance revised in 2004, the Basel 1999 guidelines on "Enhancing corporate governance for banking organisations" revised in February 2006, the OECD 2002 Corporate Governance Guidelines for Pension Funds, the IAIS and OECD 2005 Guidelines for Insurers' Governance" (OECD, 2010)

Across the Atlantic, according to the Securities and Exchange Commission, risk oversight by the board should happen "through the whole board, or through a separate risk committee or the audit committee, for example" (SEC, 2010). Pre-crisis, where risk oversight was identified as a Board role (which was infrequent) the task was usually assigned to the audit committee. The tasks are now typically split between the Risk Committee (which theoretically has a forward looking, predictive nature) and the Audit Committee (which is more traditionally focused on the reporting of past events).

The Committee of Sponsoring Organisations of the Tredway Commission (COSO), as a part of their Thought Leadership program, produced guidance for risk oversight for non-executive directors called "Board Risk Oversight – a progress report" published in December 2010. They say "Risk oversight is a high priority on the agenda of most boards of directors" and use the term "risk oversight" to describe the board's overview and monitoring of the firm's risk management practices, "including policies, processes, people and reporting" (COSO, 2010). But US regulators have not so far involved themselves in more detailed prescription of the roles and processes of risk committees, as has been the case in the UK.

4.4. WALKER REVIEW

In the UK, the Financial Services Authority commissioned the Walker Review of Corporate Governance in UK Banks and other financial industry entities as a consequence of the Global Financial Crisis and collapse of Northern Rock. The Walker Review was published in November 2009 and was very critical of the FSA's role in the run-up to the crisis and its failures to oversee corporate governance within the banks.

The main contribution of the Walker Review was to encourage the full institutionalisation of board-level risk committees as separate from audit committees. According to the Walker review, "serious deficiencies in prudential oversight and financial regulation in the period before the crisis were accompanied

by major governance failures within banks." Sir David Walker emphasised both the lack of sufficient prudential oversight and the lack of attention paid by regulators to corporate governance weaknesses.

Building on the aforementioned corporate governance regulation that was already in place, the Walker review investigated governance in the UK banking industry and focused attention on risk management and specifically on the contribution made by risk committees. More concretely, Sir David spoke about *risk oversight* in an unprecedented way. The Walker review, to illustrate a simple point about emergent importance of oversight, uses the word "oversight" 61 times in 174 pages. And it is also evident that he develops new expectations of those who carry out the role of overseeing risk managers within a firm.

Walker suggests, for example, that a risk committee should be created in order to advise the board on the current risk exposures of the entity and its future risk strategy. In order to do that, "a dedicated NED [non-executive director] focus on high-level risk issues in addition to and separately from the executive risk committee process" is needed (Walker, 2009). This is one of the most fundamental contributions of the report that had serious repercussions for those major financial institutions that did not have board risk committees at the time. Walker's suggestion made the separation between risk oversight and risk management explicit because non-executives, who oversee from above, by definition cannot be managing.

According to the International Corporate Governance Network, "Risk oversight is defined as the board's supervision of the risk management framework and risk management process. Risk management is distinct from risk oversight, as it is a responsibility of a company's management team" (International Corporate Governance Network, 2010). This distinction between risk management and risk oversight is more explicit than any definitions given by the FSA where it is assumed that the meaning is known.

Walker further recommends that risk committees should be supported by a CRO "with clear enterprise-wide authority and independence" (Walker, 2009). This observation appears to have been consequential on how risk oversight is done in

practice because it suggested that non-executives should be more directly involved in the risk management process, thus bringing non-executive directors closer to the business and giving them more responsibility for business processes. Indeed, a number of organisations (e.g. HSBC and Lloyds Banking Group in banking and Prudential and Zurich in the insurance sector) have gone further and included the CRO on the board of directors which has given CROs more visible power than had been the case previously.

Additionally, Walker explained that a "materially increased" involvement of board directors in risk oversight is required, and an increased time commitment from NEDs. The suggestion to "materially increase" risk oversight implies that engagement in risk oversight is something that can be measured and changed. Moreover, Walker recommended that responsibility should be allocated for oversight, which implies that not only is oversight measurable, but also that there are thresholds of what constitutes success and failure; the board risk committee is to blame if it is not succeeding. The fact that the board risk committee has responsibility over risk oversight also allocates ownership of the process to them, because they are now accountable for it. The Walker review narrative also implies that oversight is a good thing and that more of it is better. One could argue, however, that without a clear explanation of what oversight means, and how it is expected to enhance risk management, it is not obvious that increasing it will improve firms or make boards more efficient.

Walker also noted in his review that 'ideally, corporate governance and regulation of a financial entity should be mutually reinforcing' (Walker, 2009). This observation suggests that regulators and agents of corporate governance should support each other, thus it brings regulators closer to the business process itself as they oversee the internal overseers more tightly. The FSA responded that "review of governance will now involve more intensive work", including more thorough oversight of the "effectiveness of governance and risk management" (FSA, 2010b). In the FSA's response, when discussing the responsibilities of the Chief Risk Officer (CRO) and the Board Risk Committee, the Authority mentions "oversight" in three out of ten points for the description of the CRO's role and six out of seven

points in the description of the Board Risk Committee. This demonstrates an increased regulatory interest in oversight in corporate governance. The practice implications of that enhanced focus are explored later.

4.4.1. POST-WALKER

After the Walker review (and also possibly affected by Turnbull), the FSA's discourse changed significantly and it began to discuss oversight in terms of more in-depth firm-level corporate governance: "Regulators and legislators have focused on internal control issues as a policy response to crises, […] The monitoring role of the board of directors, which forms the apex of the internal control system of an organisation, has been emphasised" (Spira & Page, 2010). The FSA responded to Walker's suggestions in a consultation paper "Effective corporate governance: Significant influence controlled functions and the Walker review" in January 2010 and agreed with Walker that that "the board risk committee should have responsibility for oversight" (FSA, 2010b).

The FSA's guidance also enhanced the importance of the role of the CRO within the organisation, i.e.: "Alongside an internal reporting line to the CEO or CFO, the CRO should report to the board risk committee, with direct access to the chairman of the committee in the event of need" (FSA, 2010b).

Another relevant institution with a role in developing regulatory practice in corporate governance is the Financial Reporting Council (FRC) - the "UK's independent regulator responsible for promoting high quality corporate governance and reporting" (FRC, 2015). The "Combined Code" of 1998 was updated by the FRC into the "UK Corporate Governance Code" (FRC, 2010b) in June 2010 (and the following years). The FRC's responsibilities cover the whole of the public companies sector, but 2010 update could be interpreted as a response to the explosion in attention that corporate governance and risk oversight gained as a result of the financial crisis and the failures that Walker observed in November 2009.

Following the implementation of the FRC's "The UK Corporate Governance Code" published in June 2010, the Financial Reporting Council (FRC) began to publish annual updates (FRC, 2011b) on developments in the UK's corporate governance and the effect the code has on it. In October 2010, the FRC produced a thorough explanation of the reasons for improving the corporate governance codes, pointing out that "Regulation should begin with strong corporate governance" (FRC, 2010a).

In the policy statement that the FSA produced in September 2010 after taking into account feedback to their January 2010 consultation paper, the FSA suggests that "even where no risk committee exists, the firm should consider appointing someone to be accountable for risk at the firm, with the governing body retaining responsibility for risk oversight" (FSA, 2010a). Here, once again, the fact that someone is responsible and accountable for risk oversight implies that oversight can be measured against some objective criteria, although such criteria would be challenging to codify and are not explicitly specified in any of the FSA's publicly available documents.

Compensating for the fact that corporate governance shortcomings were a commonly agreed significantly contributing cause of the global financial crisis, this area became the focus of the FSA's work in the following years. In the initial consultation paper of January 2010, the FSA lists a number of criteria for good corporate governance and the Board's "evidence of active oversight through the regular scrutiny and challenge of management information" (FSA, 2010b) is one of them. The fact that the FSA now requires oversight to be "active" and "evident" demonstrates the development of the concept of oversight towards becoming something real and tangible because firms should be able to record it and demonstrate how active it is in an auditable way. As a consequence, this also leads to an increased demand for people who are seen as responsible for overseeing risks and for demonstrating the evidence of oversight.

In January 2011, the FSA shifted focus of attention from broader issues of risk governance towards the narrower field of operational risk, and published a guidance note titled "Enhancing frameworks in the standardized approach to operational risk"

(FSA, 2011), which says that "the board of directors could approve policies developed by senior management" thus stating that is it the board's role actively to oversee management's actions in that area.

Following that, the Financial Reporting Council conducted research into board-level risk oversight by interviewing a number of financial institutions, and published a report "Boards and risk" in September 2011. One of the conclusions in the report was that "there has been a step change in the Board's focus on risk in the last few years […] This conforms to the emphasis in the revised Code on the Board's responsibility for strategic risk decision-making" (FRC, 2011a). In addition the report also explains "the ownership and day-to-day oversight and management of individual risks were rightly the responsibility of executive and line management, rather than the Board" (FRC, 2011a). This explanation emphasises the difference between the functions of executive and non-executive management – while the Board's role is important in ensuring management is successfully managing risks, the Board is not expected to get involved in daily operations and the running of the business on a granular level. FRC thus defies oversight in terms of what it is not (not granular involvement) rather than in terms of what it actually is.

4.5. Individual Responsibilisation

> "The corporate governance of large banks was characterised by the creation of Potemkin villages to give the appearance of effective control and oversight, without the reality" (UK_Parliament, 2013).

As the above quote shows, the UK Parliamentary Commission report on banking standards, published in June 2013, was highly critical of the failures of corporate governance in the financial sector, explaining that "both the financial crisis and conduct failures have exposed very serious flaws in the system of board oversight of bank executives and senior management" (Parliament, 2013), with the underlying notion that focusing on boards will improve the rest of the organisation.

The Parliamentary Commission also noted that while the composition of bank boards had changed since the crisis, no disciplinary actions had been brought against individual directors whose actions (or inactions) had been a prime cause of losses to shareholders and, in the case of banks rescued by the government, taxpayers.

There are many reasons why boards might eventually fail, as indeed there are many definitions of failure, and whilst the goal of this chapter is not to make a normative judgement on the success of bank boards in the crisis, it is useful to explain as a matter of reference the common perceived problems of corporate governance in general and of risk committees in particular.

Roberts et al observe that "Through successive rounds of governance failure, the non-executive has been the target of both blame and reform", and explain that agency theory has been influential as when NEDs are "a target of blame, agency theory assumptions suggest the dangers of too close a relationship between executive and non-executive directors and the capture and collusion that this might imply" (Roberts et al., 2005).

While the distance between board oversight and executive management was emphasised throughout the regulatory documents at that time, over time there has been a shift in tone when it comes to making the board more accountable for their oversight responsibilities, including individual accountability. For example:

> "The behaviour and culture within banks played a major role in the 2008-09 financial crisis and in conduct scandals such as Payment Protection Insurance (PPI) mis-selling and the attempted manipulation of LIBOR. However, under the statutory and regulatory framework in place at the time, individual accountability was often unclear or confused. This undermined public trust in both the banking system and in the regulatory response" (PRA, 2014).

The phenomenon of focusing on individual accountability, exemplified by the quote above, could be seen as the regulator delegating responsibility for good regulation to the regulated, similar to the classic agency relationship where principals have to delegate to agents in order to be able to perform their principal duties. One of the ways in which this individual 'responsibilisation' is manifested is

the regulatory "Approved Persons Regime", which makes NEDs 'Controlled functions'. I am borrowing Power's term 'responsibilisation' of directors that he explains is "intended to activate them as corporate agents of self-organisation, through which new variants of financial auditing and assurance services can operate" (Power, 2000).

The FSA finalised the Approved Persons regime in March 2001, but prior to the global financial crisis it was primarily oriented at 'responsibilities of senior management' and those interacting with customers. After the crisis, the focus shifted towards deeper control of non-executive directors who exercise an external oversight role over the internal business practices. Power, speaking about audit, explained "audits generally act indirectly upon systems of control rather than directly upon first order activities" (Power, 2000). Regulatory control over NEDs can be seen here as a similar mechanism, as regulators focus on the 'enforced self-regulation' systems of governance and on the overseers rather than on the business itself.

In 2009, the FSA explained regarding the "focus on senior management responsibility and oversight", that they expected "to see more cases where individuals, especially those holding significant influence functions, are subject to enforcement action" (FSA, 2009a). In fact it has proved difficult to mount cases against individuals, and very few have been held accountable for their failings, a point which has been regularly made by politicians and in the media. That has caused regulators to try different approach to accountability, and to sharpen the definition of individual responsibility. One major shift was that post-crisis, the FSA started focusing on 'fitness' and 'competence' of people in "Significant Influence Functions", not just their 'propriety', and "between October 2008 and January 2010 had conducted 332 interviews, rejecting 25 applicants" (Black, 2010).

In April 2013, FSA was split into the Prudential Regulation Authority (PRA) and the Financial Conduct Authority (FCA). Banks, insurers and major investment firms are thus now dual regulated. In July 2014, PRA issued a consultation "Strengthening accountability in banking: a new regulatory framework for individuals", as a part of the response to the Parliamentary Commission on Banking

Standards (PCBS). The "Strengthening accountability in banking" policy statement was finalised in July 2015, and implemented new 'Senior Manager and Certification Regimes' that are intended to "require firms to allocate a range of responsibilities to these individuals and to regularly assess their fitness and propriety" (PRA, 2015d), and ultimately aim at a "change in culture at all levels in relevant authorised persons" (PRA, 2015d). Regulators also carry out the so-called 'governance reviews', and are able to implement additional capital requirements (PRA, 2015a) if governance is deemed to be deficient.

The Parliamentary Commission on Banking Standards, also likely influenced by the lack of regulatory discipline over individual board members who have failed to exercise due oversight, also suggested a reversal of the burden of proof:

> "The proposal to reverse the burden of proof for imposing regulatory penalties on Senior Persons in certain circumstances would make sure that those who should have prevented serious prudential and conduct failures would no longer be able to walk away simply because of the difficulty of proving individual culpability in the context of complex organisations" (UK_Parliament, 2013).

The Walker Review had made a similar suggestion:

> "Regulators should have greater capability to reverse the burden of proof and say that a senior executive who had been involved in a palpable failure would be struck off unless he could show that he had been effective, diligent and challenging in seeking to avert that failure" (Walker, 2009).

In response to the Parliamentary Commission on Banking Standards, the government legislated to allow the regulators to apply a new senior management regime which incorporated the idea of a reversal of the burden of proof. In other words, in future Directors and senior managers may be held personally responsible for regulatory breaches if they could not demonstrate that they took adequate steps in advance to guard against such breaches. The new regime was announced in March 2015:

> "The policies announced today are significant and will make it easier for firms and regulators to hold individuals to account" (FCA, 2015).

Financial Conduct Authority goes on to explain that:

> "Under the Presumption of Responsibility, when a relevant/authorised firm contravenes a relevant requirement then the Senior Manager with responsibility for the management of any of the firm's activities in relation to which the contravention occurred is guilty of misconduct" (FCA, 2015).

While it is not obvious that a 'reversal of proof' case could succeed in court, it is evident that the level of accountability is increasing, and that at the time of writing the regulators are still working on defining responsibilities of the board: e.g. in May 2015, the PRA published a "Corporate governance: Board responsibilities" consultation paper. The consultation process is due to finish in September 2015. In the draft statement, PRA demonstrates its expectations relating to 12 items, including, in this order:

- Setting strategy
- Culture
- Risk appetite and risk management

In order to demonstrate the regulatory priorities, it might be worth noting that culture came higher on the list than did risk appetite and risk management. This could be seen as part of the 'compliance-oriented approach to regulation' described by Power as relying "increasingly on the self-organising capacities of organisations", where the directors have emerged as "regulatory agents" (Power, 2000), forced to "acquire responsibility for internal control and risk management" (Power, 1999). In a similar way that audits were described by Power (1994) as shifting power as they enhance "the transparency of individual and corporate actions to those parties who have an interest in the nature and effects of those actions" (Power, 1994), regulatory demands shift responsibility for regulation from the regulators to the boards, who are thus held accountable for failures of compliance.

The regulatory focus on governance and on NED oversight more specifically manifests itself through boards being responsible for Risk Appetite and Risk Culture – the 'objects' of governance. On culture, the document explains that "The board should articulate and maintain a culture of risk awareness […]. The non-executives have a key role to play in holding management to account for embedding and maintaining this culture" (PRA, 2015c) – this allocates the responsibility over risk culture to the Board. Additionally, the board is given responsibility over risk appetite:

> "The business strategy should be supported by a well-articulated and measurable statement of risk appetite […] which is clearly owned by the board. The PRA will expect to see evidence of this active oversight of risks according to the risk appetite" (PRA, 2015c).

These terms will be used throughout the thesis, and are also the objects through which regulatory responsibilisation of the board manifests itself, therefore the following section provides an explanation of both, including current regulatory and academic views about them.

4.5.1. RISK APPETITE

Defining and controlling the firm's risk appetite could be seen as an important object of oversight: "Risk appetite linked to strategic planning is part of the board's risk-taking oversight" (Andersen et al., 2014), and is in theory at the core of business practice in financial institutions (IRM, 2015) because it is needed to allocate capital (KPMG, 2013a), which is fundamental to the whole functioning of the institution. Power explains that the prescriptive way to look at it is that, in theory, "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. The model is that of a thermostat which adjusts to changes in environment subject to pre-given target temperature" (Power, 2009).

According to the Financial Reporting Council's Corporate Governance Code, the Board "has responsibility for an organisation's overall approach to risk management and internal control", which includes "determining the nature and extent of the principal risks faced and those risks which the organisation is willing to take in achieving its strategic objectives (determining its 'risk appetite')" (FRC, 2014a). While the idea is that NEDs set risk appetite, in practice to do so they require information from within the firm, together with suggestions from management about what they should focus on.

In order to set and monitor risk appetite, the Board (Chapter 5), according to the interviewees, receives a vast amount of information (Chapter 7) from within the business (Chapter 6). The production of the Risk Appetite statement is an interactive process that happens across different layers of organisation, all the way up to the NEDs who approve the final statement. Difficulty arises at once, however, as there is an inherent ambiguity in the manifestation of Risk Appetite - while Risk Appetite is the purest outcome of information production, serving as a conclusion to a laborious process of gathering and analysing strategic priorities and risks, and is the condensed goal of information, at the same time the risk appetite statements are in theory meant to determine the priorities with the organisation and thus influence what the information flows will be like. It is not possible to assert, therefore, that there is a 'pure' process uncorrupted by the potentially conflicting interests of principals and agents who are competing for capital between different parts of the firm.

4.5.1.a. History

The origins of risk appetite, as a focus of regulation and oversight, are not clear. Financial firms have traditionally controlled credit allocation (Bernanke, 1983), or business volumes generally, but the terminology of 'risk appetite' is relatively new. The earliest mentioning of risk appetite indemnified was in the 1989 Global Capital Markets KPMG report that said a number of institutions "have

embarked on fundamental reviews – starting with a re-assessment of their risk appetite" (Peat, 1989), which by its tone implies its prior existence. And according to a library search, "Risk Appetite" was not in the title of any publications until the 2000 Journal of Finance article "Does Option Compensation Increase Managerial Risk Appetite?" (Carpenter, 2000). Andersen et al (2014) observe, vaguely, that "Relatively recently, that is, around 2008, the extended corporate governance communities taken up the use of the term 'risk appetite', encouraging and mandating boards to formally approve their firm's 'Risk Appetite Statement'" (Andersen et al., 2014).

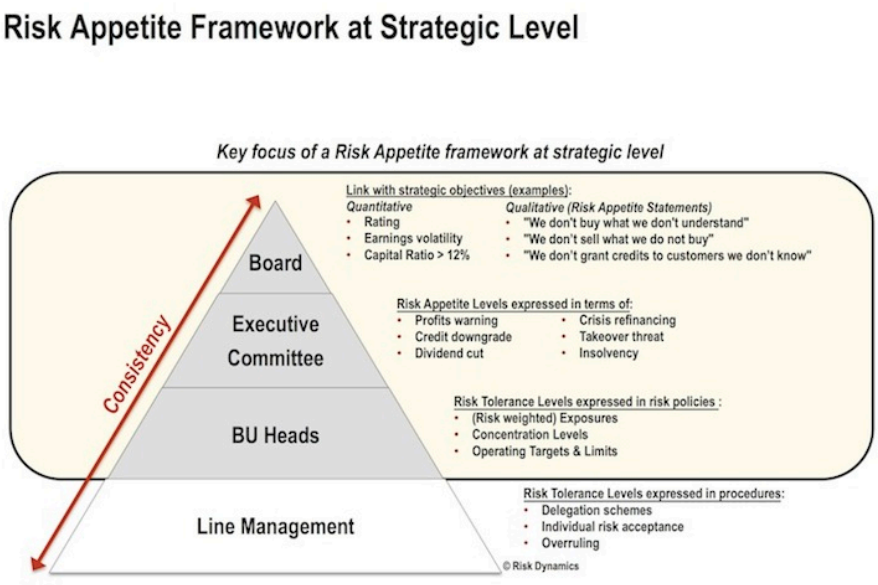
Arguably, one might link its existence to the concept of Enterprise Risk Management, because risk appetite is a way of assessing how much risk the firm is willing to take, which is later monitored through the theoretically broadly-encompassing ERM framework. ERM, in turn, emerged "in the late 1980s as an extension of hazard risk management" (Hampton, 2009). One of the reasons risk appetite frameworks are used widely across organisations, is their characteristic of being a common discussion point for conversations within business, similarly to Hall's (2010) observation about the role accounting information plays in organisations: "the strengths of accounting information vis-à-vis other information at a manager's disposal […] include its aggregation properties and its role as a common language to facilitate communication among managers with different backgrounds, experience and knowledge" (Hall, 2010).

4.5.1.b. Definition

While risk appetite is intended to operate throughout an organisation, the role it takes on varies. At the board level, risk appetite is the language of strategy and oversight of its implementation, where the board is intended to set the culture for how risk appetite is treated. At lower hierarchical levels risk appetite becomes manifested through individual risk tolerances and operational limits. Risk appetite, even within one firm, could thus be seen as having multiple meanings, which are in

theory ideally complementary to each other in ensuring complete risk coverage throughout the ERM framework. Figure 4.1, prepared by one of the risk consultancies, describes a typical approach that in theory is taken to risk appetite in a bank, and also demonstrates one of the numerous representations of risk appetite by consultants.

FIGURE 4.2: RISK APPETITE FRAMEWORK



(RiskDynamics, 2014)

It can be seen from the depiction above that the appetite may take on different roles at different strategic levels, and may also contain both quantitative and qualitative elements. The quantitative elements can be measured, by definition. Table 4.2 shows that a set of data can be produced within a bank to support the quantitative component, but that process involves critical judgements, which may be made by management; and NEDs may find it difficult to assure the quality and relevance of such data without independent support. It is also clear that the data will vary over time. Credit quality will deteriorate in an economic downturn, so ex ante and ex post risk appetite may well differ. The information assembly process must therefore be dynamic and timely to allow adjustments to be made.

TABLE 4.2: MAIN CATEGORIES OF RISK IN A TYPICAL BANK AND THEIR MEASURABILITY

Risk	**Measurability**	**Measures**
Market	High	Volatility experience
Credit	High	Default history, loan losses, non-performing loans
Operational	Medium	Error rates, IT system checks
Reputational	Medium	Staff/customer surveys, hiring patterns, turnover
Regulatory	Medium/Low	Incidence of fines/penalties
Legal	Medium/Low	Case records, other similar litigations

Qualitative risk appetite definitions are even more problematic, as was frequently mentioned by interviewees at various organisational levels. As Power describes, "Although, COSO (2004) envisages the possibility of 'qualitative' understandings of risk appetite, the dominant conception is that of a quantitative benchmark such as a target level of financial capital to be maintained [..] as a kind of self-insurance against shocks and adverse events" (Power, 2009).

"[Boards] are beginning to break free from regarding appetite solely as a 'thing' to be measured and to recognise it as a dynamic construction involving values and the situational experience of a multitude of organizational agents" (Power, 2009) – the currently common Three Lines of Defence governance structure (that separates the risk accountabilities between functions within the business units, risk management, and internal audit) might be seen as an answer to that, as it creates a slightly more clear and visible distribution of roles and 'ownership' of risk.

The NEDs interviewed (see Chapter 5) were all members of risk committees, and are likely therefore to largely rely on judgements made by the second line of defence (see Chapter 6). While the second line of defence (independent risk managers) are supposedly 'independent' of business unit management, the Risk Management function still ultimately reports to the CEO. NEDs, as some of them

have explained during the interviews, lack a fully independent source of judgement which would allow them to challenge a second line assessment, unless they commission an external evaluation, which reports directly to them, a practice which is currently very rare.

4.5.2. RISK CULTURE

> The 2014 UK Corporate Governance Code defined Corporate Governance as "what the board of a company does and how it sets the values of the company" (FRC, 2014b).

The first prominent mentioning of culture within the context of oversight is in November 2004, when Kari Hale, FSA director of finance strategy and risk, said that "management of operational risk is […] in its infancy, and management of them is – to a large extent – about culture and appropriate management *oversight*" (FSA, 2004). The fact that Hale said in 2004 that risk management is "about culture and appropriate management oversight" is notable because using the word "appropriate" implies that there are some objective criteria and thresholds of what constitutes appropriateness and what does not. However, these criteria might be difficult to evaluate or even categorise, because of how imprecise the ideas are. The regulation has not published a clear definition of the meaning of 'appropriate' in this context. A statement about appropriateness without any explicit mentioning of the requirements leaves a lot of space for interpretation and thus also creates a potential domain of interest for management and risk consultants who fill in this gap between regulatory suggestions and practical implementation.

Ashby et al consider risk culture a challenging topic to research because "many, though not all, of these habits and routines are not readily visible, even to organisational participants themselves" (Ashby et al., 2012). This might explain why the regulatory concept of "appropriateness" of risk culture is so vague - it is not just difficult to monitor from outside, but even problematic for actors internal to the organisation to see and understand.

Despite this inherent vagueness, the link between oversight and organisational culture is a recurring theme in a number of later discussions about risk oversight. Ashby et al find that unlike a lot of emphasis on "values and the need to change mindsets, we learned of risk culture work streams with more of an emphasis on improving oversight structures and information flows, including performance metrics for risk and good compliance" (Ashby et al., 2012). One could argue that just as culture is at the heart of oversight, effective oversight structures and information flows are at the heart of operationalising risk culture.

According to a chairman of one of the UK's largest banks:

> "Regulators are constantly asking about risk culture, and emphasising that it's the Board's responsibility to set the tone from the top. But it's hard to know how to measure culture, and to work out what interventions by the Board would make a difference" (Interviewee_12, 2014).

Indeed, probably as a response to both the internal problems and potentially the regulatory pressures, culture became absorbed into the conduct risk agenda that is now discussed and controlled. Some boards even have dedicated board committees explicitly responsible for it. - for example, HSBC's "Conduct & Values Committee" established in January 2014 is given responsibilities including "[doing] business with the right clients and in the right way, is a responsible employer, acts responsibly towards the communities" (HSBC, 2015).

The process of responsibilisation that regulators are now articulating could be seen as is transforming the nature of boards by recruiting their members in support of regulators and their objectives. Board risk committees then become responsible for the firm's risk appetite and risk culture. In order to be able to perform their role, they need support structures and information suppliers within the firms to give them the information. This wide scope of responsibility, and risk tolerance close to zero (Davies & Zhivitskaya, 2014) on the part of the regulators, poses additional challenges in executing the NED role.

4.6. CONCLUSION

This chapter has traced the convergence of corporate governance and financial regulation, and demonstrated the increased overlaps and increased attention to risk from both sides. The financial regulators have in particular increased their focus on corporate governance within firms over the last several years: the financial crisis has been widely interpreted as showing that the "self-regulation" of financial institutions without close regulatory oversight has failed. That may in part be the result of inadequate time spent by NEDs, and in part by a deficient understanding of the nature of risk in modern financial markets (shared by firms and their regulators). Moral hazard may also have played a role - large firms were considered 'too big to fail' and their funding costs were lower as a result, giving them cheap money with which to speculate. Whatever the reason, financial stability was not protected strongly enough, resulting in a financial crash and severe costs imposed on taxpayers who, in the UK and elsewhere, were obliged to rescue a range of banks deemed crucial to the functioning of the economy.

Looking at it from the agency perspective, financial institutions have two major categories of principals – regulators and shareholders. Regulators are principals because public authorities might need to bail the firms out should something go wrong, and that will cost money to taxpayers (who are thus the principals of the Prudential Regulators), and might also cause inconvenience to customers (who are the principals of the Financial Conduct Authority). Shareholders are the owners, and thus they are principals in the classical definition of the term. Traditionally boards are supposed to represent the shareholders' interests. However, in the changing regulatory environment, boards also have to pay a lot of attention to the regulators due to the process of responsibilisation.

Reacting to the governance failures in the financial crisis, the Walker review in the UK, and other reviews internationally, focused on non-executive directors and their role. Sir David Walker criticised the way the boards treated risk management before the crisis and suggests that it should be different in the future: "In the past,

some bank boards may have seen risk oversight as a compliance function essentially designed to meet regulatory capital requirements with minimum constraint on leveraged utilisation of the balance sheet […] Such attitudes should have no place in the proper governance of risk in future" (Walker, 2009). In the final report, Walker outlines several suggestions of what needs to be done in order to increase board-level engagement in the risk oversight process.

As a response to the financial crisis and the Walker review, regulators started looking more closely risks within financial institutions as a part of a tightening of regulation (higher capital standards were the most costly response), and created a new concept of risk in FSA's discourse compared to that in the earlier years. When the FSA started monitoring risk-taking within the firms, they focused primarily on risk governance and risk management structures.

To summarise, there has been a significant change in the way regulators speak about oversight and frame their interest in risk. First, their focus was on risk to their own objectives. Only later did they begin to talk about risk to firms themselves. Now it is multi-faceted, and involves at least three components:

- risk to regulators' objectives
- risk to individual firms
- risk to the system as a whole.

Possibly due to the level of complexity of the term, in most of the publications mentioned above "oversight" is not defined explicitly, even though it can carry several meanings and, as has been shown, is used within somewhat different contexts. While oversight is difficult to explain, there is no doubt that in theory assigning ownership of oversight to different actors within financial networks is meant to empower them to interface with various aspects of risk management within the firms and perform supervisory roles. In this sense, efforts by the regulator to measure and improve the effectiveness of oversight without providing clear criteria about what exactly it means, could be explained by the regulator delegating the task of determining 'good practice' to the boards themselves as they perform their role.

Overseers are not management, and they are by definition outside the activity that is overseen. Risk oversight does not contradict, but rather complements the concept of risk management because risk management continues to be done within firms, with oversight being put above it in the governance structure. The focus in recent years has been on overseeing the overseers – specifically, the regulators oversee the non-executives' oversight of the financial institutions. The regulators' focus on non-executives led to a change in the governance paradigm from NEDs being remote from the business to them actively participating in the risk oversight process. The lack of clarity about where risk management stops and risk oversight begins, is one of the defining features of this field.

These regulatory developments demonstrate a very distinctive path of regulating firms through the regulation of their governance; however they could also have chosen to focus on other things such as e.g. making the firms smaller. Instead, regulators have been closely involved with the way firms organise themselves to manage risk, specifying committees and particular responsibilities for specified individuals, as well as ways of organising risk oversight. They have required the adoption of:

- Board Risk Committees, where they also now require particular ways of working (more in Chapter 5)
- Three Lines of Defence (more in Chapter 6)

As we shall see in the following chapters, firms are finding it challenging to deliver this agenda and meet regulators' enhanced expectations, which are threatening the traditional approach to corporate governance, in which NEDs and executives are part of a collegiate board collectively responsible for promoting shareholder value. A new tension between executives, and non-executives strongly influenced by regulatory expectations, has been introduced into the corporate governance of financial firms.

CHAPTER 5: Board RISK OVERSIGHT

5.1. INTRODUCTION

Increased regulatory interest in the boards of directors has been discussed above. This chapter investigates *how do risk committee members understand and operationalise their risk oversight roles*? "While the details vary, there is wide consensus that the directors' role is one of oversight, not to undertake operational duties" (Andersen et al., 2014). Regulators now expect Boards to oversee the lines of corporate defence, and in order to do so they receive information from those lines with the help of information intermediaries, as we will see in the following two chapters.

The Walker review in November 2009 discussed the need for risk committees in the UK financial institutions. Six years later, regulators are still attempting to define board responsibilities, as evidenced by the PRA's current call for responses on the consultation paper "Corporate governance: Board responsibilities" (PRA, 2015b) that is due to close in September 2015. In this consultation document, an effective board is defined as one which "understands the business, establishes a clear strategy, articulates a clear risk appetite to support that strategy, oversees an effective risk control framework, and collectively has the skills, the experience and the confidence to hold executive management rigorously to account for delivering that strategy and managing within that risk appetite" (PRA, 2015b). Even though the document is about the board as a whole, not specifically about risk committees, a substantial part of the definition of an effective board has to do with risk. This might be interpreted as a way of prioritising the Risk Committee which is usually tasked with these jobs.

The increased focus on risk committee responsibilities is hardly surprising: it has been observed that corporate governance change is often pre-empted by exogenous shocks (Fligstein, 1993; Zietsma & Lawrence, 2010) - the trigger for many changes related to risk committees can be traced to the financial crisis. The emergence of board risk committees can be interpreted as an additional indicator of the increased significance of risk management in the sphere of corporate governance, in line with the overall responsibilisation of boards and increased emphasis on risk. This chapter discusses the role of board members, and, specifically, of NEDs in the risk oversight process with the help of qualitative research methods (primarily interviews conducted in the summer of 2014).

As mentioned in the introduction and the methodology chapter, the primary research objective when approaching the NEDs was a general one: to understand how NEDs make sense and define their role in risk committees, and what they see as the key challenges in that process. Risk oversight, unlike risk management, might not necessarily be about making decisions, but instead about observing the way these decisions are made. After desk research and a number of informal conversations with NEDs, an interview protocol was created (see Appendix II) that focused around sense-making in terms of the role definitions, accountabilities and interactions with other stakeholders, such as managers who can be seen as agents and regulators who can be seen as principals.

Focusing on the financial sector Andersen et al explain that: “The trouble at firms that were previously lionized as corporate exemplars, such as Citibank, Deutsche Bank, Royal Bank of Scotland and UBS, revealed widespread weaknesses in how boards undertook the oversight of risk in their enterprises” (Andersen et al., 2014). Part of the diagnosis of the reasons for the global financial crisis points to inadequacies in risk oversight, primarily caused by two factors, namely (a) the limited time boards spent on risk, and (b) the lack of relevant expertise on the part of the board members involved. Regulators then responded to these failures by requiring special, focused Risk Committees in addition to the already existing Audit Committees and by insisting on the presence of individuals with relevant experience

and expertise. This in turn led to the problematisation of the relations between risk committees and the rest of the board, as the risk committees are now responsible both to the board and the regulator.

The rest of the chapter is structured as follows: first, an overview of the historical evolution of the NED role is discussed, followed by an overview of the main points of criticism of Board-level risk oversight, primarily based on the academic reference points. It is followed by a discussion of the way audit and risk committees differ from each other. Role ambiguity and the key relationships are then presented based on the interview findings, followed by a discussion of those findings. These themes arose based on the reading of interview transcripts, partially pre-disposed by the questions asked and partially by the thematic grouping of the answers. The overarching arising themes include the contrast between aspired and actual oversight practices, as well as observations about how NEDs make sense of the vagueness of oversight.

5.1.1. HISTORICAL EVOLUTION

> "Boards have been a subject of interest in many disciplines beyond economics and finance, including accounting, law, management, psychology, and sociology" (Adams, Hermalin, & Weisbach, 2008)

Studies of the nature of the NED role are primarily survey-based, and the outcomes vary significantly based on the sample size and particular questions asked; to demonstrate the variety of responses across different years – i.e. a survey by Mace as early as 1971 found that NEDs see their role as "advice and counsel" (Mace, 1971), while Demb and Neubauer found that 45% of NEDs think their job is to "oversee and monitor top management" (Demb & Neubauer, 1992), and 26% of their survey respondents said their role primarily involves succession and top management hiring and firing. The variation of survey responses about the nature of the NED role indicates inherent role ambiguity, and also shows that it has changed over time.

While corporate governance phenomena (including the role of NEDs) are researched by different disciplines, there is not much academic work on risk committees specifically, due to the fact that they are a relatively new addition to the corporate governance world. However, parallels with the literature on the longer established audit committees can be drawn and many of the general issues that boards face are also directly relevant to Board Risk Committees.

Theorising about corporate governance goes as far back as Adam Smith, who wrote that "The directors of such companies, however, being the managers rather of other people's money than of their own [...] Negligence and profusion, therefore, must always prevail" (Smith, 1776). The goal of this section, however, is not to trace the historical evolution of corporate governance in general or the NED role in particular, but rather selectively to highlight the parts of recent history that led to the creation of Board Risk Committees as they are now. Bhimani observed that "Adherence to financial reporting standards is regulated by audits which provide a mechanism for assuring compliance. Standards of compliance in respect of corporate responsibility and governance have more recently also been the subject of legislation" (Bhimani, 2008) - board risk committees present a case of such a governance mechanism.

In the l970s, Mace discussed the decoupling of board responsibility and actual activity, and found that boards neither "ask discerning questions" nor "select the CEO" (Mace, 1971). One of the first reports that reacted to the several corporate governance scandals was the 1987 Treadway report on fraudulent financial reporting in the US sponsored by COSO[12]: in order to do so, it identified "attributes of corporate structure that may contribute to acts of fraudulent reporting"

[12] COSO - The Committee of Sponsoring Organizations of the Treadway Commission – is a commission composed of five industry bodies and includes Institute of Management Accountants (IMA), the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors (IIA), and Financial Executives International (FEI) – and is "dedicated to providing thought leadership to executive management and governance entities" (COSO, 2014)

(Treadway, 1987) and issued good practice guidelines for Management reports and for Audit Committees.

Millstein and MacAvoy trace the history of the corporate boards in the US and find that "The evolution of boards from managerial rubber-stamps to active and independent monitors has been in large part the result of efforts to address or avoid serious performance problems associated with managerial entrenchment", and that since the 1990s boards have become more closely aligned with the shareholder interests, which in turn has allowed them to "enhance value to shareholders" (Millstein & MacAvoy, 1998).

Caldwell emphasises that when it comes to the responsibilities, "Boards of directors are not expected to unilaterally identify, analyse, mitigate and monitor enterprise risk. Rather, boards must oversee the risk management systems and processes and continuously review the associated outcomes and planning" (Caldwell, 2012). The role is thus primarily monitoring and control, rather than implementation of corrective actions, which is instead done by the management, and these two roles should be "clearly delineated" (Caldwell, 2012). Similarly, according to Deloitte's "Assessing Enterprise Risk Management" report published in May 2009, "management has the primary responsibility for assessing enterprise risk, the audit committee and the board may have an active role in overseeing the process and in understanding management's response to the identified risks" (Deloitte, 2009). This distinction is critical because while management assesses and manages risks, the oversight role is in place in order to confirm the reasonableness of these actions, and this very specific role of the audit committee or the board risk committee became institutionalised through regulatory requirements.

Before the crisis regulators focused little attention on board composition, and the checks they did on board members were limited to "fitness and propriety", which amounted to checking court records for evidence of criminal activity, fraud, and bankruptcy. Since the crisis, regulators have been shifting their focus so as to add consideration of competence for the particular roles that the board members will perform. This focus is expressed in different ways in different places. The US regulators have long had a requirement for at least one "financial expert" in the

audit committee, for example, but do not interview directors in advance of appointment as the UK regulators do.

The UK now goes further and defines a number of Significant Influence Functions (SIFs): for example, the Chair of the Risk Committee is viewed by the regulators as a person exercising significant influence over the firm and is thus required to be approved as a part of the role, which involves being subject to formal interviews under the system of 'close and continuous' supervision. Regulators are holding boards to account for their effectiveness, and indeed the new 'reversal of the burden of proof'[13] regime for bank boards in the UK further emphasises the responsibilities Boards now have for risk oversight, as was discussed in Chapter 4. The 'close and continuous' interviews include detailed questions about the board's competence to perform these particular roles. Some candidates are rejected, but while there is anecdotal evidence of that fact, no statistics are published. There stricter requirements on board composition have meant that, according to Grant Thornton's annual corporate governance report, "Board structure and composition continues to be the most common reason for non-compliance" (GrantThornton, 2011). Other common criticisms of the board-level risk oversight are discussed in the following section.

5.1.2. FAILURE OF RISK OVERSIGHT

During the last two decades there has been an increased emphasis in both the regulatory sphere and in academic thinking on directors' independence (Clarke,

[13] "Senior bankers will be presumed guilty until proven innocent under strict new rules proposed by British regulators seeking to hold individuals accountable for bank failures", which is a result of the 'presumption of responsibility' rule by the Financial Conduct Authority which requires senior managers to demonstrate that where a firm is guilty of misconduct they "took such steps as a person in their position could reasonably be expected to take" to avoid it happening" (Schuffham, 2015).

2007; Eisenberg, 1999; Lin, 1995). This increased emphasis on independence has, over time, led to a growing proportion of independent directors on boards (Gordon, 2007), and it is notable that "most directors today are very part-time" (Carter & Lorsch, 2013) due to the fact that the role was designed to be part time and independent in order to avoid a close alignment of financial interests which would create a bias in their judgements. There is, as it is commonly acknowledged, a limited pool of potential candidates for those high-level jobs, who are typically involved in other boards and/or executive managerial (or sometimes academic) positions alongside being on boards.

In addition to the part-time nature of the job, Bainbridge & Henderson mention that "the reasons boards continue to struggle include inadequate time, misspent time, inadequate information, improper skill sets and insufficient incentives" (Bainbridge & Henderson, 2014) and yet there are now regulatory requirements addressing each of the these reasons listed by Bainbridge and Henderson: for example, regarding time commitment, board members need to demonstrate to regulators that their other activities leave them adequate time for the role. As of July 2014, they cannot be involved in more than one executive directorship and two NEDs or four NEDs at the same time (according to the EU Capital Requirements Directive IV). Noting this, the goal of this chapter is not to provide an in-depth assessment of regulatory developments, which were touched upon in the previous chapter, but to focus instead on the NED perspective, which is relevant because NEDs are key actors in shaping oversight, but are also a group that is difficult to research due to the limitations of access. As some argue that increased regulatory demands lead to boards being "more focused on compliance with standards and regulations than they are on obtaining a competitive advantage" (EY, 2013a), this, in turn, might mean that boards risk having less time to spend on strategic decisions and supporting management.

The limited time spent on the work of an individual board due to other commitments of their members might be further amplified by an inherent information asymmetry – citing Bainbridge and Henderson once again, "independent directors are […] by definition outsiders", which means that

regardless of their best efforts, they "do not have the time or the mandate to challenge management's judgments except as to a discrete number of issues" (Bainbridge & Henderson, 2014). Thus, the question of cause and effect might remain unanswered, since it is possible to argue both that the inherent information asymmetry (of which they are aware) makes NEDs less engaged and thus causes board members to spend less time trying to bridge their knowledge gaps or, as the inverse of that, that the fact that they spend less time being involved means that the information asymmetry remains an issue. These problems of information asymmetry will be discussed in more depth in Chapter 7, but it is useful to note for now that the challenges of information and information flows are related not only to this asymmetry, but also to its amount, since both receiving too little and too much information can be problematic. The use of the terms "too little" and "too much" is inherently simplistic and does not take into account whose appetite towards the depth of information counts.

The problem of "improper skill sets" noted by Bainbridge and Henderson can be linked to the other two issues discussed earlier – that the NEDs are outsiders to the business and thus do not possess deep firm-specific knowledge and also that they might not be getting sufficient information from within the business to learn about its functioning and its vulnerability. Since February 2014 the US Federal Reserve requires all risk committees in major financial US institutions to include at least one "risk management expert", who is defined as someone having "experience in identifying, assessing and managing risk exposures in large, complex financial firms" (FED, 2014). Comparatively few people have such qualifications, and firms are finding it hard to meet this requirement given the relative immaturity of risk management as a specific discipline. The Institute of Risk Managers (IRM), The Professional Risk Managers' International Association (PRIMA), and Global Association of Risk Professionals (GARP) are three of the major international organisations that provide numerous qualifications: Project Risk Manager, Financial

Risk Manager, and Energy Risk Professional among others[14]. Financial Risk Manager Qualification, for example, was established by GARP in 1997, and currently has over 30,000 practitioners worldwide (GARP, 2015).

An additional difficulty arises when one takes into account that tasks of risk committees go beyond financial risk management, and involve a wider skill set such as for example PR, politics, IT resilience and others that might require other qualifications. The problem of improper skill sets related to the complexity of risks in financial institutions was observed by de Larosière: "Many boards and senior managements of financial firms neither understood the characteristics of the new, highly complex financial products they were dealing with, nor were they aware of the aggregate exposure of their companies" (de Larosière, 2009).

Even though the tangible impact of boards is difficult to observe, when things go wrong board members are in theory held accountable: "The directors of Enron and WorldCom, in particular, were held liable for the fraud that occurred: Enron directors had to pay $168 million to investor plaintiffs, of which $13 million was out of pocket (not covered by insurance); and WorldCom directors had to pay $36 million, of which $18 million was out of pocket" (Adams et al., 2008; Klausner, Munger, Munger, Black, & Cheffins, 2005). Lehman Brothers directors, however, have not so far paid anything, and regulators on both sides of the Atlantic have found it difficult to attach responsibility for failures in the financial crisis to individual board members, as evidenced for example by the FSA reports on the failures of the Royal Bank of Scotland, which states e.g. "the fact that a bank failed does not make its management or Board automatically liable to sanctions. A successful case needs clear evidence of actions by particular people that were incompetent, dishonest or demonstrated a lack of integrity. […] Errors of commercial judgment are not in themselves sanctionable unless either the processes

[14] For more information, please see: https://www.theirm.org/training/all-courses.aspx and https://www.garp.org/frm/

and controls which governed how these judgments were reached were clearly deficient, or the judgments were clearly outside the bounds of what might be considered reasonable" (House of Commons, 2012). That complexity in responsibility attribution has, as has been discussed earlier, led to legislative change in the UK which tightens the responsibilities of NEDs.

Another frequent criticism is that NEDs devote too little time to their responsibilities, but the main way that NEDs are intended to add value is, by definition, precisely by being distant from the main business process and by introducing an external perspective to it. So it is not self-evident that regulators can expect that spending more time within the business will lead to a better outcome. Additionally, there is very limited empirical evidence about whether the somewhat normative ideas discussed above hold true in the case of board-level risk oversight.

Additional problem which is not clear is whether the issue is too little time spent, or time spent looking at inadequate information. According to The Walker Report, "if performance systems do not assure an adequate information flow to the NEDs, no amount of financial industry experience among the NEDs will right the situation" (Walker, 2009).

With audit committees pre-dating the establishment of risk committees, and having formal responsibility over risk until recently, it makes sense to explore risk committees with reference to the audit committees. In July 2015 audit committees' role in risk oversight, especially in non-financial firms, is still crucial:

> "Most boards delegate oversight of risk management to the audit committee, which is consistent with the NYSE rule that requires the audit committee to discuss policies with respect to risk assessment and risk management. Financial companies covered by Dodd-Frank must have dedicated risk management committees" (Wachtell, 2015).

An example of audit committee taking responsibility over risk oversight prior to the crisis (and it being common practice) could be demonstrated by this explanation of the failures of RBS during the financial crisis by the FSA:

> "Although, in the pre-crisis period, RBS did not have a formal Board Risk Committee (as subsequently recommended by Sir David Walker's report), risk issues were the responsibility of the Group Audit Committee (GAC). This was not out of line with standard practice at the time" (House of Commons, 2012).

5.2. AUDIT VS RISK COMMITTEES

When audit committees were first widely introduced in the UK as a result of the Cadbury report published in December 1992, these committees were already mandatory in all firms based in the US, which is why many multinational firms based in the UK already had them; thus, the publication of the Cadbury report, when all stock exchange listed firms were effectively required to have these audit committees in place, did not create a seismic change. In 2009, the Walker review led to a more dramatic trajectory of change: many firms had risk committees in place before they were formally required. In firms outside the financial sector, it is still common practice to have one single committee responsible for both audit and risk. The Walker review suggested: "The audit committee's terms of reference should be expanded to include oversight of the risk appetite and control framework of the company; in complex groups where this would overload the audit committee, it may be more practical to establish a separate Risk Committee dedicated to this function" (Walker, 2009).

Within the governance framework of financial institutions, audit committees were typically also responsible for risk, though the term did not always appear in their charters. One likely reason why Audit committees used to be responsible for risk is that following the ENRON scandal in 2001, the core of which was serious accounting misconduct, the audit committee took over the oversight of similar issues; furthermore, "some governance experts, sensitive to the need for risk management in non-accounting areas as well, defined audit committee responsibility with enough breadth that non-accounting risks tended to get swept in" (Young, 2010). In the UK, audit committees were thus used to be responsible both for audit and risk issues up to November 2009, when the regulators' response to

Walker review changed the rules at financial institutions: these institutions have had to separate the two functions and, although executive risk committees were often in place before, oversight of risk has been elevated to the highest level of board governance since the Walker Review.

A relevant observation is that "Although the board's emphasis on risk is expanding, the audit committee's focus, with regard to specific areas of risk, seems to be narrowing" (Steffee, 2011). Caldwell compares the role of the board in risk oversight to the role of the audit committee: "The audit committee does not prepare financial statements, draft disclosures, or maintain the system of internal control. Rather, the audit committee bears responsibility for overseeing" (Caldwell, 2012).

Corporate governance operates through committee structures, and bank boards nowadays typically set up all of the following committees: Audit, Risk, Nomination and Remuneration. Some banks now also have their Risk Committee sub-divided into further NED committees (e.g. reputational and compliance risks might be separated from financial risks) which are then even more focused, and add yet another level of complexity to the corporate governance regime. While the work of Nomination and Remuneration committees is often closely linked with the work of Audit and Risk committees, it falls outside the primary focus of this thesis so will only be mentioned in relation to their relevance to the Audit and Risk committees.

There is a theoretical overlap between the roles of the Risk committees and Audit committees, but their tasks differ substantially: according to the Walker review, in the simplified form, the role of the risk committee is forward looking while audit committees are typically more institutionalised and are seen as backward-looking. This makes the risk committee more ambiguous, since Management Information that the boards receive is primarily based on backward looking data, but one of the challenging roles for a Risk Function within the firm is to aid the forward looking process, e.g. through stress testing, scenario planning, emerging risk assessment etc. rather than purely reporting on past compliance with risk appetite, past credit defaults or operational losses. The data behind such

exercises is inevitably based on assumptions and judgments, and therefore has a substantial subjective element.

The overlap between risk and audit committees became even more significant with the introduction of risk-based audit in "Effective Internal Audit in the Financial Services Sector" published by the UK Chartered Institute of Internal Auditors in July 2013: this report encourages audit committees to become more future-oriented, thus blurring the line between the roles of risk and audit further. During my interviews, the overlap was not raised as a problem and it was not mentioned at all when the committees' responsibilities were discussed. However, the previous general distinction of audit as backwards looking and risk as forward-looking not only still remains but also appears frequently when these committees are spoken about, both in literature and by the committee members themselves. The forward-looking focus also means more advanced calculations in order to aid judgment, which also means, in turn, that arguably the responsibilities and boundaries of the risk committees are less clear and less defined than those of audit committees. For example, practice differs on the types of risk that should be covered by the Risk Committee. Operational risk is sometimes included, or may be handled by a separate Operations and Technology Committee, as is the case in the investment bank I observed.

DeZoort discusses the paradox that the audit committees faced in the 1990s as they were "a monitoring mechanism expected to assume expanded oversight responsibilities in an environment where its credibility and effectiveness are increasingly in question" (DeZoort, 1998). This observation is similar to the development of the risk committees' ability to perform their oversight role, as shown in the earlier section on criticism of board risk committees.

Abbott et al studied the audit committee oversight of internal audit and found a strong positive association between the audit committee's oversight of internal audit and internal audit's "internal-controls-based activities" (Abbott, Parker, & Peters, 2010). Rephrased, their finding means that a stronger and more involved

audit committee directs the attention of internal auditors towards internal oversight – assuming these findings would also hold for risk oversight, Abbott et al make a strong case for more active risk committees. However, as noted above, internal audit is a small part of the audit committees' agenda, given that audit committees must also approve the annual reports as well as public statements regarding performance forecasts.

The UK Parliamentary Commission on Banking Standards summarises the role neatly: "the audit committee has clear responsibility for oversight and reporting to the board on the financial accounts and adoption of appropriate accounting policies, internal control, compliance and other related matters. […] This vital responsibility is essentially, though not exclusively, backward-looking" (UK_Parliament, 2013). Regarding the scope of the audit committee responsibilities, it includes approving the statement of accounts and confirming that everything is as described in accordance to the rules; additionally, Audit committees interact with external auditors and receive their reports on the firm's accounting practices and indeed external auditors may raise concerns about financial management directly with the Audit committee, without management present. The Internal Audit function has a direct reporting line into the Audit committee, but NEDs do not 'head' Internal Audit, as that is the role of Chief Internal Auditor: according to one Chair of Audit Committee, only 15% of their agenda is driven by the work of internal auditors.

Keizer warns about "the false sense of security […] that risk oversight is "under control" simply because it has been assigned to a designated risk committee" (Keizer, 2010). That 'sense of security' inevitably varies from firm to firm, as does the division of the roles of risk and audit committees. An illustrative example, Table 5.1 demonstrates the division of responsibilities in Morgan Stanley (chosen at random as one of the top investment banks):

TABLE 5.1: RISK AND AUDIT COMMITTEE CHARTERS

Risk Committee[15]: Oversight of -	**Both**	**Audit Committee[16]: Oversight of -**
Risk Tolerance	Risk Management	Relationship w/ Independent Auditor
Capital, Liquidity, Funding	Coordination with Management	Internal Audit Department and Internal Controls
Chief Risk Officer	Coordination with Other Board Committees	Financial Statements, Audit and Disclosure
		Compliance with Legal and Regulatory Requirements

Looking at terms of reference of a risk vs. audit committee above, it is clear that while there is an overlap on overseeing risk management, the rest of the responsibilities are distinctive. When overseeing risk management, both committees "Review or discuss, as and when appropriate, with the Chief Risk Officer, the head of the internal audit department and other members of management, the Company's guidelines and policies that govern the process for risk assessment and risk management" (Morgan_Stanley, 2014a, 2014b), but the Audit committee is required also to "Review the major legal and compliance risk exposures of the Company and the steps management has taken to monitor and control such exposures" (Morgan_Stanley, 2014a) while the risk committee should "Review at least quarterly the major risk exposures of the Company and its business units, including market, credit, operational, liquidity, funding, reputational and franchise risk […]"

[15] Source: Risk Committee Charter (as amended May 13, 2014) - https://www.morganstanley.com/about/company/governance/pdf/rcchart.pdf?v=20140513

[16] Source: Audit Committee Charter (as amended October 31, 2014) - http://www.morganstanley.com/about/company/governance/auditcc.html

(Morgan_Stanley, 2014c). The Risk committee also receives reports "from the Head of the Internal Audit Department regarding the results of risk management reviews and assessments" (Morgan_Stanley, 2014c).

When it comes to the fundamental different responsibilities of typical Risk Committees compared to those of Audit Committees, the former involve overseeing capital soundness (regulatory requirements, e.g. Basel for banks), overseeing stress tests, and ensuring that the firm has sufficient liquidity to cover increased demands in stressed conditions. In recent years, Recovery and Resolution Plans (colloquially known as living wills) have also become a major area of responsibility; living wills are highly technical forecast documents that explain how the financial institution would expect to wind down its assets and liabilities (without causing distress to the rest of the financial system) in the event of it no longer fully meeting regulatory requirements, while still trading. Risk Committees also oversee the pillars within the risk divisions, which typically are credit, market, and operational risk[17].

Some NEDs serve as members on both committees, and when it comes to granular issues within how to oversee risk management, for example, Chairs of risk and audit committee need to decide on the division of labour, and also typically, the Chair of Risk Committee sits on the Audit Committee and vice versa. Terms of reference create the official story about the operationalisation of risk and audit committees – they could be seen as a part of the ritual, in line with one NED who observed "I've been chair of risk committee for several years and I don't look at the

[17] The role of the Risk Committees does, as expected, differ between financial institutions. For example, the 2013 Parliamentary Commission on Banking Standards report observed that: "In HSBC, the Group Risk Committee is responsible for 'advising the Board on high level risk-related matters and risk governance and for non-executive oversight of risk management and internal controls (other than financial reporting). In Barclays, there are three different risk committees responsible for different aspects of risk: the Board Conduct, Reputation and Operational Risk committee; the Board Financial Risk Committee; and the Board Enterprise Wide Risk Committee". (UK_Parliament, 2013)

terms of reference" (Interviewee_02, 2014), while another NED amplified that point further by explaining that communication with regulators and others in the field are much more useful than the terms of reference.

It would appear that, internationally, UK corporate governance practice has led the way in this area, but risk Committees conceived on similar lines are now common in other jurisdictions: in December 2009 in the US, the Securities and Exchange Commission (SEC) issued enhanced proxy disclosure rules in which it was emphasised that boards are responsible for risk oversight and "additional disclosure would improve shareholders' understanding of boards' roles in risk-related practices" (Deloitte, 2010). The aim of these increased disclosure requirements is to "require companies to explain how the board administers its risk oversight function, […] and how employees responsible for risk management report to the board" (Deloitte, 2010). Partly as a consequence of this rule, and partly due to enhanced interest in risk oversight shown by other regulators, most US banks have now also introduced separate risk committees, which operate along similar lines to those in the UK. In the Eurozone, practice varies, but the larger banks (e.g. Deutsche Bank and Credit Suisse) also operate risk committees of a similar kind, as they are now deemed to be best practice.

For Audit Committee members, the expertise requirement in the US has been defined as "past employment experience in finance or accounting, requisite professional certification in accounting, or any other comparable experience or background which results in the individual's financial sophistication, including being or having been a CEO or other senior officer with financial oversight responsibilities'' (BRC & NYSE, 2002). The Federal Reserve requirement for expertise of risk committees is "borrowed heavily from Securities and Exchange Commission and national securities exchange requirements applicable to Audit Committees" (Dentons, 2012).

Indeed, the forward-looking approach could be seen as one of the reasons why risk committees are now seen by the board members as the most challenging committee to be a member of, which is demonstrated in a survey carried out by the

Per Ardua recruitment consultancy (Per-Ardua, 2014), in which 80 per cent of respondents said the Risk Committee was now the one committee which worried them most. The concerns expressed by the surveyed NEDs referred to the high degree of responsibility needed in order to understand the business and to the difficulty of forward-looking judgment based on what remains primarily internal information. An additional challenge could be that it might not always be clear what these different bits of required information are.

The internal audit function does in theory provide an independent support for Risk Committee in their oversight role of the risk management function; however, there is no Risk Committee equivalent to the external audit function, which is intended to act as a source of independent information and, to a degree, of assurance to the Audit Committee. The independent information and assurance aspect of the external auditors' work also means that the Audit Committee receives good practice feedback about how other firms are organised, while similar information is not yet a routine part of the Risk Committee's world. The insurance company observed as a part of this research has now, however, commissioned an external report on the organisation and staffing of risk function in competitor firms.

Risk committee members are an important part of the fabric of oversight that this research attempts to examine: so their views of, as well as their approach to, their role are significant. However, since Risk Committees in their current form are a relatively recent creation, there is little 'off the shelf' data on the subject. The difficulty of research access to boards is commonly recognised (Daily et al., 2003; Roberts et al., 2005), however whilst regulatory and corporate governance guidance leaves much to be defined, the semi-structured interviews were carried out in order to discover more about the live experience of the Non-Executives.

5.3. Role Ambiguity and Conflict

Based on the discussion of the historic evolution in the previous section, it is evident that the nature of the non-executive role has changed since the financial crisis and the Walker Review. As an example of this, according to a NED in a risk committee in a major retail bank:

> "After the financial crisis, it was much more on the question of safeguarding the future of the organisation, […] what would it take to make sure the organisation survived and could then emerge from the financial crisis? You know, that was not the focus beforehand." (Interviewee_01, 2014)

When describing his NED role, a chairman of the risk committee of a major insurance firm explained:

> "It's a bit like flying a plane; it's 95% boredom and 5% sheer terror".
>
> (Interviewee_06, 2014 on being a Non-Executive director)

This interviewee continued to explain that while he has no actual management power, she does still have an important steering role:

> "I have no management role. As a Board Risk Committee you have no management role. You cannot take a decision […] everything is governance and oversight. And you use influence and respect I guess and the positional power to get management to do stuff" (Interviewee_06, 2014).

Acknowledging that risk committees receive information from the risk management function, and also that many of them have held executive managing positions earlier in their careers, the Board-level interviewees were asked about balancing the management and oversight roles.

5.3.1. DISTANCE BETWEEN MANAGEMENT AND OVERSIGHT

Even though in theory, and indeed by definition, NEDs have no management role; in practice, due to their knowledge and experience, as well as the increasing expectations placed on them by regulators and shareholders, it can be difficult for NEDs to remain entirely separate from the management process. Their role is to oversee management, but the fuzzy borderline in the spectrum between oversight and execution is not always clear, and is affected both by dynamics within the firm and by regulators. As one interviewee explained this struggle:

> "The regulators now expect you to be far more closely involved in the business than you were before. So the line itself between accountability and the traditional role of the non-exec on the board and the management has shifted and finding your place in that is very difficult" (Interviewee_12, 2014).

And, indeed, when asked about their role, interviewees' answers fell along a spectrum, ranging from absolutely no intervention in managerial tasks to stepping in and managing when needed, although one particular interviewee advocated a very critically separate view, i.e.:

> "One of the phrases I rather like is kind of "nose in, fingers out" type of concept of the NED" (Interviewee_02, 2014).

Therefore, interaction with management was frequently explained as more than merely getting management to "do stuff", but actually involved non-executive support and certain encouragement of managerial actions as well:

> "A good board is one that challenges and does all of that sort of stuff but also is supportive and helpful when you want them to be, provided what you're doing is sensible" (Interviewee_05, 2014).

Together with encouragement and support, challenge while remaining distant from the executive decisions is another aspect of the NED role:

> "One of the biggest challenges is to be challenging, understand the business, understand the people, stand back but then not get involved in the execution" (Interviewee_08, 2014).

One interviewee, who was a CRO in one firm before taking on the role within the Risk Committee in another, also pointed to the inherent difficulty of transitioning from a high-level management role into a Non-executive oversight role:

> "If you step back from being a hands-on manager and you simply just want to step in and say being prescriptive, you have to be very careful not to be prescriptive in areas - that's management responsibility. You can suggest, you can encourage" (Interviewee_09, 2014).

This polarity indicates that oversight could be defined negatively as 'not management', as the role of the NEDs according to the above quote is not management. Yet countering the prior point, another interviewee explained the value of providing hands-on interventions:

> "You would only intervene and manage if there was an absolute crisis and something was going wrong. And what you really have to do if the executive are not managing the organisation effectively, you have to decide whether with appropriate advice and coaching and whatever it might take, you can get them to manage the place effectively. If you can't, you have to change them. I mean that's ultimately what you have to do as a non-executive" (Interviewee_08, 2014).

Regardless of which strategy a NED chooses to follow, one interviewee acknowledged that the act of 'standing back', even if she wants to, might not always be easy due to the external pressures:

> "There's a little bit of a drift in financial services for the non-execs almost to be given executive responsibilities. There are times when you're almost as though you are an executive. You can't be an executive, you cannot be an executive" (Interviewee_04, 2014).

A less expected theme that arose during the interviews was a clear need for balance as part of the dual nature (colleagues vs. overseers) of the Non-Executive role in a unitary board structure (which is the case in the UK, where a single board

of directors includes both executives and non-executives). In the US, where typically the only executive on the Board is the CEO who is often also the Chairman, the Board has more clearly an oversight role distinct from management than is the case in the UK. Non-executives in London are, based on the interviews, seen as colleagues of the executives, with shared responsibility for both the strategic decision and the success of the company, but they are also a part of the oversight of management – and very explicitly so in case of regulated firms.

They are conscious of the need to balance the contradictory aspects within the role of being close enough to management in order to fulfil a role of a colleague, while distant enough to oversee, and generalist enough to identify broader issues while remaining enough of a specialist to understand issues at the required depth. This double dichotomy might make it seem an 'impossible job'. Interviewees were particularly conscious of the need to be both critical and supportive:

> "It's very important not to try to second-guess the executive […] you have to go there, you're there to operate governance which means challenge and it means sometimes criticism. But it's also about encouragement and development" (Interviewee_05, 2014).

To summarise, no 'standard' definition of the oversight role emerged from the interviews, mainly due to the fact that the definitions were full of contradictions and drew a complex multifaceted picture of the role. Respondents were preoccupied by the difficulty of defining a role which provided a useful check and balance on management without crossing the line into executive action, the main elements of such a role seemingly including a) an ability to stand back from day-to-day pressures, b) a longer-term frame of reference, and c) a focus on shareholder and regulatory interests, which may differ from those of management incentivised by near-term revenue and profit targets. But the borderline between risk oversight and management is clearly problematic for some NEDs at this point in the evolution of Board Risk committees.

5.3.2. *What is Success?*

With an unclear definition of the role, and a complicated balancing act on the managing and oversight spectrum, a question about what constitutes success was asked. Criteria for success is a particularly complicated theme for NEDs, especially in cases of risk committees, where success might mean the lack of bad things happening and is therefore less easily auditable than in case of a profit-generating functions. This ambiguity in how to measure success makes the *process* of reaching decisions a regulatory and practitioner focus. Interviewees often defined success as an outcome of the group as a collegiate process, not at an individual level. The factors that were frequently identified by the NEDs as leading to success were:

(1) Experience
(2) Diversity
(3) Group decision making

From the interviews conducted it is evident that NEDs believe there is certain value in introducing a perspective on the business not informed by direct day-to-day involvement in management, but one perhaps influenced instead by experience gained in different types of financial firms or in non-related industries.

> "You need to have people that have been experienced […], that have worked in industries and have a depth of knowledge in at least one or two businesses, so not superficial knowledge but a depth and have very senior level jobs in one or two different businesses/industries" (Interviewee_09, 2014).

Whilst appreciating background and experience, diversity is seen as a requirement in ensuring that the group dynamic results in the best possible outcome. Most UK boards have now formally committed to at least 25% female representation, following a 2011 review by Lord Davies (Davies, 2011). NEDs also see added value in group decision-making on risk, which is inherent in the introduction of a committee responsible for such wide array of tasks:

> "Good non-executives hunt in packs […] it's groups of them rather than individuals is when they're most successful" (Interviewee_06, 2014).

The value of collegial decision-making is also manifested through the ability to interact effectively outside the boardroom in support of the formal interactions:

> "So you have to be able to not quite build alliances, that implies too formal a situation, but you have to be able to work with people effectively to test whether what you're believing is right" (Interviewee_06, 2014).

And yet, though they identify these potentially positive elements of non-executive involvement in risk oversight, NEDs also acknowledge the difficulty of proving that the quality of decision-making, and that of risk management itself, has been materially enhanced as a result. Moreover, it have been suggested that NEDs are conscious of the need to show evidence of their own success and performance in addition to overseeing others:

> "You're never quite sure what contribution you make because risk management's kind of the dog that doesn't bark […] if you do your job well, fewer bad things happen. But who's to say whether they would or they wouldn't have? It's quite difficult to attribute success, it's difficult to measure success" (Interviewee_03, 2014).

In the absence of solid evidence applicable to their own roles, NEDs tend to emphasise their personal experience and the importance of judgment by the people who directly manage risks in the business, implicitly accepting the limitations of oversight as opposed to management; therefore, this interpretation attempts to show

that oversight actively influences the quality of management, rather than merely passively observing or second-guessing it. Counter-factual evidence is difficult and it requires time, since much of the success of risk management lies in the nature of problems avoided – things not happening – rather than in identifiable positive actions, although over time it may be possible to calibrate the influence of risk committees. When it comes to studying the way risk committees influence the businesses they are involved in, a parallel could be drawn to the way risk officers in Hall et al. (2015) gain influence. Hall et al. demonstrate two separate aspects of gaining influence: (1) interpersonal connections, and (2) toolmaking - the way risk managers "adopt, adjust, and reconfigure tools that embody their expertise"(Hall, Mikes, & Millo, 2015). The remainder of this chapter focuses on the connections – both interpersonal and formal - that NEDs described to be crucial to their role, and the following two chapters look at the organisational structures in place to ensure NEDs are able to successfully exercise their oversight role. This thesis does not specifically analyse the tools.

On the opposite side of this argument, while there was a variety of definitions of success, which implies that success is a rather vague category, definitions of failure (and examples of difficult experiences they had to face) always turned out to be rather more specific and narrower, and these examples of difficult situations were always related either to changing and appointing people (usually management, but also other board members) or to events that happened as a consequence of the financial crisis, or of control failures within firms, or both.

With all this in mind, it is safe to say that one provisional conclusion, albeit a broad one, from the interviews is that risk committees are still 'feeling their way' towards a stable definition of their roles and functions. It can also be argued that this stability will never come and indeed that risk committees might be an inherently ambiguous and unstable practice that is built on competing tensions. Some of these tensions might also still be present in audit committees and the board as a whole. Within the risk committees particularly, although they are now a fixed feature of the corporate landscape, at least in the financial sector where regulators mandate their existence, the practical outcomes of their work remain unclear and their impact on

the effectiveness of risk management has not yet been demonstrated. The following sections examine how NEDs define their role, starting with a discussion of how they perceive their accountability and key relationships.

5.3.3. LENGTH OF TENURE

Another current issue within the area of corporate governance that is directly related to success (and independene) is the length of tenure that may be deemed appropriate for NEDs. On the one hand, having recruited a successful risk committee member the firm might be interested in retaining that person for as long as possible, but, on the other hand, there is a risk that NEDs who are close to the business for too long may actually also become dangerously close to the executives and therefore lose their independence, in this case understood as their ability to bring an external perspective to decision-making[18]. Yet knowing the business well and understanding the people within the business are important in order to be a successful non-executive, and requiring people to move on after a few years could mean that the depth of interaction and business-specific knowledge will eventually be lacking. This tension between the need for independence and what is necessary in order to succeed in being a non-executive is a sensitive issue.

Currently, in the UK, NED tenure is effectively limited to 9 years, typically divided into three three-year terms, with the requirement for a special review after 6 years to justify a third term. Companies are entitled, under the 'comply or explain' provisions, to implement longer terms if they can produce a clear justification for it, but very few do so. Therefore, this bias towards rotation gives firms an easy option to remove people, but at the same time it introduces an element of difficulty for these companies to keep the people whose ongoing contribution would be most

[18] The issue of independence vs. tenure also is similar to the debates commonly discussed in relation to external auditors.

valued – this is, in effect, an asymmetrical option. Other comparable countries, notably the US, do not impose such arbitrary limits on tenure and, as a result, NEDs tend to stay longer in their posts, albeit as Risk Committees are a relatively recent introduction it is not yet clear how practice will evolve in this area. NEDs are also aware of this tension, and take diverse positions on the advisability of term limits:

> "Nine years is quite a long time […] six years is probably a bit better but then nine years is an absolute maximum. But I don't think it's just about the nine years, I think it's about the whole dynamic of the board. So it's not just how long each individual person sits there, it's that the board is regularly refreshed and it only takes one new person […] the whole dynamic of the board can change" (Interviewee_08, 2014).

While others explicitly link length of tenure to success and disagree with the currently imposed nine-year limit saying that:

> "I would define [success] as acquiring the respect of the business you know, the top team and other people. And really feeling you've acquired that. Really feeling you know the business. Unfortunately when you really do that they chuck you out because it's the nine-year rule" (Interviewee_02, 2014).

Term limits apply to directors of any given age, but the age of directors has also become a controversial point since the financial crisis and the failure of firms with some very elderly directors. A study of the 25 largest European banks by Nestor Advisers which compared the banks that failed and survived after the crisis shows, for example, that "there seems to be a discernible relationship between age and failure: the departed board directors were on average 66.5 years old while those of the survivors are 61" (Nestor, 2009), and while this study does not make any causal claims, this correlation might be worth noting and exploring further with a larger sample longitudinal study. In the UK, There is no mandated retirement age, but most companies include a cut-off in their own policies, often at age 72.

A difficulty companies face is that the increasing time commitment required of NEDs works against the appointment of senior executives from other companies,

which is pushing firms towards the appointment of retired executives. On the other hand, the nature of the financial system is changing rapidly, making the experience of retired executives less relevant. The only proposed solutions to this dilemma are (1) the development of a cadre of 'mid-career' non-executives, but they remain rare, or (2) continuous education requirements on NEDs. In practice, regulators are promoting the second option. In the UK they now interview NEDs to assess their knowledge of new regulatory developments, for example, and require companies to develop training programmes for their NEDs, which are designed in particular to ensure that they remain aware of regulatory developments.

5.4. ACCOUNTABILITY AND KEY RELATIONSHIPS

A Wachtell Lipton[19] memo on Risk Management and the Board of published in July 2015 observes: "2014 Annual Corporate Directors Survey reported that 84% of directors believe there is a clear allocation of risk oversight responsibilities among the board and its committees, which represents a modest increase from the prior year, but over half of these directors suggested the clarity of the allocation of these responsibilities could still be improved" (Wachtell, 2015). This shows there is still some uncertainty about the role they play and about how the various committees position themselves on the boundary between oversight and management. Admittedly, this uncertainty might be inherent in the nature of the NED job, and is also partially the case for audit committees, but it is more extreme. That uncertainty about the nature of the Risk Committee's work is particularly evident in the case of answers to questions about accountability, as well as about the relationships within and outside the firm between the Risk Committees and other sources of power and decision-making.

[19] Wachtell Lipton is a New York law firm which is one of the leading corporate governance advisors to major US companies.

The lack of clear definition regarding the expectations, success criteria and accountability of risk committee NEDs imply that they are, in a way, part of the phenomenon of experts competing "for visibility and voice in the competitive landscape of management practices and ideas", because they need to establish both their role and usefulness (Guadalupe, Li, & Wulf, 2013; Hall, Mikes, & Millo, 2013), while also establishing the scope and depth. Furthermore, this need to balance the scope and depth of the role is manifested through the expectation that they will "provide public demonstrations of performance through objective measures" (Gendron & Bédard, 2006). Overall, drawing parallels to the 1990's audit quality discussion, risk management today could similarly still be characterised by "elusive epistemological character" (Power, 1999), implying that further clarification of the meaning and expectations of the roles could be needed.

While there is no lack of vague information about the role of risk committees, when it comes to the particular points about the nature of the role, the guidance is often rather weak. Moreover, role ambiguity is manifested through the question of scope (what falls under the realm of the Risk Committee – if too many things do it might become unmanageable) and also depth (how deep are NEDs expected to go before they depart from their oversight role into a management role). Successful performance of NEDs is difficult to account for, so the notion of expertise is a hinge that can be seen as holding the system together.

Roberts et al explore the roles of NEDs and suggest three linked sets of characteristics that NEDs should embrace. Specifically they state that NEDs should be: "'engaged but non-executive', 'challenging but supportive' and 'independent but involved'" (Roberts et al., 2005). This taxonomy is helpful, up to a point, but the interviews suggest that NEDs find it difficult to achieve these three balancing acts. Balancing these various aspects of the role could be seen as one of the defining features of oversight, and the variety of the interview responses to the questions about what it means to be a successful NED demonstrates that the intrinsic nature of the role can be quite ambiguous.

So, it is perhaps not surprising, against that complex and shifting background, that questions about accountability and relationships, within and outside the firm, elicit differing and in some cases hesitant answers, many of which are difficult to interpret. The three key relationships that risk committee needs to manage are discussed further in this chapter include those between the Risk committee and the top management, shareholders, and regulators respectively.

5.4.1. CRO AND MANAGEMENT

Although in practice there are many types and levels of interaction between Directors and management, both within and outside the Boardroom, the centrality of the relationship between Non-Executives on the Risk Committee and the CRO is nonetheless well understood.

To give a few examples of how interactions between the boards and other corporate governance actors can be conceptualised: Roberts et al, in their study of board members based on 40 interviews within the UK firms, distinguish between 'minimalist' and 'maximalist' board members. Minimalist ones do not get heavily involved in the firm outside the board meetings while maximalist board members "build their organizational awareness and influence through contacts with executive directors, managers and other non-executives beyond the boardroom" (Roberts, McNulty & Stiles, 2005). Roberts and Stiles explain that "The most often cited description of the division of labour between chairman and chief executive is that the former runs the board and the latter the business", and show the interaction styles between board and the management team in terms of competitive vs. complementary modes (Roberts & Stiles, 1999). While they acknowledge that while the separation between board and executives is crucial, they advocate an importance of a strong relationship between two.

During the conducted interviews, there was an identifiable sense of dependency on the CRO in order to be a successful Chair of a risk committee[20]; this is explained by the fact that the information flows towards the risk committee come primarily from within the organisation. Therefore, it is not surprising that almost every interviewee emphasised that it is crucial to maintain a close link with the CRO, as well as the importance of establishing mutual respect and trust

> "Formally I would see him one-on-one at least once a month. In reality I would see him probably once a fortnight/once a week. I'd certainly speak to him at least once a week. […] A good chair of the risk committee has a great relationship with the chief risk officer. You have to build a relationship of trust" (Interviewee_06, 2014).

This important factor – keeping deep and open channels of communication between the CRO and the Committee – is always seen as a crucial one, with trust and interpersonal relationships at the core of it. To add to this, non-executives also tend to be particularly conscious of the danger of being kept in the dark and uninformed about problems and disputes within management and they see the CRO as their 'eyes and ears' within the company structure:

> "I don't think I could imagine myself sitting on a board in a company where there was any sort of mistrust or secrets going on between the executives and the board" (Interviewee_05, 2014).

This is the reason why, the importance and intensity of the relationship with the CRO was repeatedly mentioned during the interviews, as manifested through frequent meetings and interactions which go beyond those related to formal risk committee meetings. It is worth noting that this relationship (with the CRO) was explained as a multi-faceted relationship as well as one which included a number of different ways of interacting. Here, these interactions are summarised in the

---

[20] For example, one of the interviewees said that in order to be successful, a chair of risk committee needs "a good chief risk officer who can present them with the information." (Interviewee_03, 2014)

following categories which arose during the interviews, and were later organised in the chronological order: pre-approving board risk committee discussion points; de-briefing after the meetings and agreeing action points; challenging and monitoring; and encouraging and motivating management.

5.4.1.a. Pre-approval and Debriefing

As shown earlier in this chapter during the discussion of the boundaries of the role, in terms of more direct involvement, NEDs are generally resistant to the idea that they might play a management role of any kind within the organisation; however, at the same time some NEDs do point to the important role they play in guiding and supporting management in general and the CRO and the senior risk management team in particular.

> "I chair the committee and I have a very intensive relationship with the chief risk officer, so I will meet with him twice a month […] Not always just him but his team as well. Either we'll be going through what we want to present at the next risk committee or we'll be going through a particular area of risk that we're trying to develop" (Interviewee_09, 2014).

Some of these meetings outside the boardroom are of a formal nature, such as the agenda approval process mentioned by this risk committee Chair in a major investment bank:

> "Before each meeting there is a formal session on the phone about the agenda where the CRO, the CFO, the Company Secretary, etc, talk through the agenda … and ask me for my views on the agenda points as well" (Interviewee_12, 2014).

But some interactions and meetings seem to be less formal and part of the process of supporting management and providing feedback:

> "I meet them before every meeting for a preparation for the meeting. […] And then I meet them after the meeting as a debrief to say what went well and what didn't go well, what actions we'd taken away and how we prioritised those actions" (Interviewee_10, 2014).

In this context there is an evident sensitivity to the risk of generating potentially dysfunctional disputes between different elements of management, while recognising that the TLD model, and the challenge role of Risk Management, may make this inevitable at times. Chairs of Risk Committees typically see it as their role to attempt to head off disputes, which might otherwise surface at the Committee or at the Board:

> "You don't want to embarrass the executives if there are mistakes or you don't want to show off, so there are some things I would just ring up the CEO and ask a question or say something's wrong, you just don't do that in a meeting. You want the meetings to be productive" (Interviewee_02, 2014).

The desire for productive interactions also included the need to balance the monitoring and motivating aspects of the role, as shown in the following section. My sample included more references to monitoring and challenging rather than to motivating and encouraging.

5.4.1.b. Monitoring vs. Motivating

> "I have a good relationship with the chief risk officer; it's horses for courses. […] I work together with him and his team very closely indeed. I have separate meetings with them and I'm kind of chief coach but also chief challenger. […] I think they would trust me to come and tell me about a problem, which is very, very important" (Interviewee_08, 2014).

Despite the great significance of the relationship between the Chair of the Risk Committee and the CRO, it is also understood that reliance solely on one individual, or indeed just on formal channels of communication, is unlikely to give a board member the full picture he or she might need. So, since tensions between the risk function and others within management are bound to surface, Board members frequently mentioned the importance of cultivating relationships with other executives, both inside and outside Risk Management.

> "I interact with the CRO and I interact with the people who work for him, the risk team. […] It's always helpful to have informal contacts with other

> members of the executive because I think when you have conversations with them about how they're reacting to what the CRO is doing or what the risk department is doing, you can get a much better more-rounded view of how things are working out. […] It's not about spying on the chief risk officer but it's about just getting another perspective" (Interviewee_05, 2014).

This interaction, with people in other functions as well as below the CRO, which is carried on in order to get confirmation about the CRO and the sufficiency of information provided, although seen as a challenge, is also perceived as a necessary condition of performing the NED role successfully:

> "There are a number of challenges; one is to develop good working relationships with the executives and also people at the next level down. Absolutely critical is the Chief Risk Officer and his staff […] the whole purpose of those relationships is not just for their sake and to have friends, but to make the passage of information to you, both formal and informal, much better. It's essentially to form an opinion as to whether you can trust management because I think if you can't trust the senior executives then probably nothing else you do really matters" (Interviewee_02, 2014).

In addition, Non-Executives recognise that the Risk Committee is likely to be kept informed more fully – and respected more – if 1) it is seen as performing a useful function and 2) it is not trying to duplicate or replace management process.

> "Trying in a sense to make the discussion more strategic than procedural, which is really difficult. It's really difficult because you will be drawn into, especially in a regulated industry, a lot of talk about our compliance processes and our documentation processes. That's an inevitable part of that world. And you know, that will crowd out the strategic discussion. So it's a real balancing act" (Interviewee_02, 2014).

This could be summarised in two key points. Firstly the Committee should perform a useful strategic function that does not in principle conflict with the management role, but rather supports it. That entails trying to ensure that the Committee continues focusing on a strategic oversight role (though that language was not always used by the Board members themselves). Secondly the Committee should provide a forum for accountability in order to make sure that risk managers have a space in which their concerns, when they have them, can be registered at the highest level within the company's governance.

The fact that the CRO can raise his or her concerns at Board level strengthens the risk management function in its debates with line management. The CRO is not obliged to raise concerns, and may choose to conceal them, but the recommended governance procedures require the committee to conduct regular private sessions in which the CRO is asked to raise any concerns: a CRO who makes a conscious decision not to do so would then be left exposed to severe criticism if an undisclosed risk were to crystallise in the future.

When it came to motivating and encouraging, this chair of a risk committee explained:

> "There's numbers but in the end organisations are bundles of human beings. And if you don't get the right human beings and you don't motivate them in the right way, you're not going to get the right outcomes. You can have sexy models coming out of your ears but in the end human beings are very, very clever and they will get round them. So if you're not motivating people properly, if you haven't got them engaged in the sort of vision then all these models eventually will be circumnavigated" (Interviewee_08, 2014).

As described above, the CRO reports to the Risk Committee, but it is clear that her career prospects, and the day-to-day effectiveness of her work, are more dependent on the relationship with the CEO than that with the Committee, as the former is of a more continuous and granular nature. Therefore, were the CEO to be dismissive of the risk function or non-executives in particular, or to be uninterested in open debate, the task would become significantly more difficult to carry out – and perhaps even impossible.

5.4.2. SHAREHOLDERS

Although most respondents were very careful to point out that they are ultimately accountable to shareholders – in accordance with company law – for the most part that accountability is indirect: Chairs and members of risk committees rarely meet shareholders directly. Chairmen of Boards do so, however, and it is also

now general practice for Chairs of Remuneration Committees to meet the governance experts of institutional shareholders. But, in addition, some companies nowadays hold "governance days" in which all the main Committee chairs, as well as the Chairman, explain the work they do on behalf of the shareholders. Yet although this may one day evolve into common practice, it is so far experimental, and shareholders have shown little interest in engaging directly with Risk Committees.

Potentially accentuated by the fact that most of the NEDs in the interview sample were involved in major global financial institutions, the practical distance between risk committees and shareholders might have been one of the core reasons why, while most interviewees mentioned the shareholders, they usually did so usually quite briefly and within the context of other categories of stakeholders; in fact, none of the interviewees pointed to any instances where their work had in practice been influenced by the views of shareholders.

> "Well the glib answer and probably the answer I would have given six years ago is the shareholders, we're shareholder representatives. I think it's a bit broader than that now in reality. I mean you know, I think you've got to take a slightly broader view of the key stakeholders, certainly the regulators want to co-opt us. I'm a bit uneasy about the extent to which they want us to be their eyes and ears" (Interviewee_11, 2014).

Possibly as a reaction to the dispersed ownership, there are now also 'proxy shareholders', e.g. ISS (Institutional Shareholder Services is a firm that describes itself as a "provider of corporate governance solutions for asset owners, hedge funds, and asset service providers. ISS' solutions include objective governance research and recommendations, end-to-end proxy voting and distribution solutions"). These firms in practice perform elements of the typical shareholder role for many institutional investors, and e.g. 'police' corporate governance compliance on behalf of the shareholders. When discussing shareholders, interviewees have not spoken about such firms. However, they did explain that their accountability to shareholders manifests itself in two ways: through management and through the regulators.

5.4.2.a. Manifested through management

When it comes to understanding NED accountability towards the shareholders, a possible argument would be to view the responsibility to shareholders as manifested through interactions with management; and, indeed, while the NEDs are ultimately trying to maintain and enhance the value of shareholders' equity, the active route to doing so passes through management, who make the practical day-to-day decisions. Therefore, shareholder accountability must also involve ensuring that management does make the right decisions.

Acknowledging that ultimate responsibility of a NED to the shareholders, one interviewee explained:

> "I think it's about the way one interacts with the management. The assumption is that the non-executive directors have a special role to play in terms of the future of the company as a whole, the long-term value of the company" (Interviewee_01, 2014).

NEDs see that their main contribution to the maintenance of shareholder value lies in ensuring that there is a strong management team in place, and in this context specifically one which is able to navigate around life-threatening risks to the business. But regulators have also begun to discuss the threat of imposing a supplementary capital requirement (Bank of England, 2014) on firms whose governance they regard as weak, the so called 'governance add-on'. Since such a requirement would have a real cost, it is intended to shape the focus on strong board governance processes, and the risk committee is a big part of that.

5.4.2.b. Manifested through regulators

Another fact that was frequently acknowledged during the interviews is that for regulated financial firms the shareholder focus must increasingly be tempered by an awareness of the interests and views of regulators acting in the public interest:

> "In order to survive as a bank after the financial crisis it was necessary to meet a whole new set of pressures […]. So the primary role of the bank remains to its shareholders but with very much a change in the focus and the intensity of the regulatory framework" (Interviewee_01, 2014).

That theoretical relationship of accountability to the shareholders was indeed frequently seen as running through the regulators:

> "You can only discharge your responsibility to shareholders by having a good and compliant … not compliant in the sense of agreeing with everything that they say but compliant in the sense of obeying rules, relationship with the regulator. So one follows naturally from the other." (Interviewee_04, 2014)

Overall, while shareholders as a category were always acknowledged, it was also noted that they are abstract and remote: in most cases too remote to be influential. It is possible to interpret the fact that shareholder interests are manifested through two different proxies - in a way, creating an image of shareholders makes the NED role possible.

In case of remuneration committees the accountability to shareholders has been formalised through the requirement to submit remuneration policies, and the remuneration reports, to an explicit shareholder vote. In a few cases, chairs of risk committees have invited shareholders to discuss their work, but there is no such formal nexus of responsibility, even though it is arguable that the activity of the Risk Committee is as, if not more, important from the perspective of maintaining shareholder value.

It seems possible that shareholders are taking some time to come to terms with the importance of the stewardship role of Risk Committees: so far they have devoted much more attention to audit and remuneration committees. One cause might be that it is harder to evaluate how well as Risk Committee has performed – business ideas not pursued due to a Risk challenge are by definition not visible externally, nor are risk mitigation measures. Audit and Remuneration Committees, on the other hand, both typically have tangible annual outputs for shareholders – an external audit and a published set of directors' pay and policies. So it is not yet clear how the shareholders could become more engaged with the risk committees, even though they arguably have a more decisive impact on shareholder value: a malfunctioning system of risk management and oversight can be fatal for a bank, as the financial crisis vividly demonstrated.

5.4.3. REGULATORS

Responsibilisation from the regulatory perspective was discussed in the previous chapter. The following section aims to understand the NED side of that process, particularly when it comes to defining the NED roles.

Interviewer: How often do you meet with the PRA[21]?
Interviewee: As often as they want.

The influence of regulators on Non-executive directors, and especially on risk committees, is now substantial. This relationship is, as the response shown above indicates, of an expectedly submissive nature. It is also the one area in which the views of respondents were at their most diverse and consensus is hard to find. This diversity of opinions might be attributable to the fact that risk committees are a comparatively new category of corporate governance and are thus still developing,

[21] PRA = Prudential Regulatory Authority. See Chapter 3 for more about the UK financial regulation.

but all interviewees agreed that the new approach taken by regulators since the start of the crisis had changed the nature of their role in a very fundamental manner. So, a typical response to a question about whether the interaction between NEDs and regulators had changed was:

> "Hugely! Until the financial crisis the regulator was an element, one among many elements. They were clearly there, everybody respected the role of the regulator but there were not … I'm trying to find the right word … The word omnipresent comes to mind" (Interviewee_01, 2014).

This increased regulatory attention also means that there are heightened expectations and pressures on the NEDs, e.g. one interviewee pointed out that:

> "I think there's a danger of expectations that you know, the regulators are full-time, the non-execs are part-time but in a way that interaction will generate more and more expectation on the non-execs as agents of the regulators to do more and more" (Interviewee_02, 2014).

Though all NEDs saw evidence of the same phenomenon of extended regulatory presence they were divided on whether this was a positive or negative development from the point of view of the effectiveness of their influence on risk management. So, when assessing the regulatory influence on board risk committees, one of the interviewees observed:

> "It is easy to emphasise what is difficult about the new system, and to be frustrated by the demands of regulators. But, overall, the introduction of a risk committee has sharpened the Board's focus on what is going on in the business, and improved its understanding of how vulnerable the bank is to outside events. So it must be seen as a net positive, in spite of everything" (Interviewee_12, 2014).

Interaction with regulators was also seen as a multi-dimensional issue that resulted in varied responses: some were quite positive and appreciated the value of information sharing and support that regulators give, while others were pensive about the confrontational nature of interaction within the boards which is accentuated by the separation between the NEDs and executives which in turn leads to possible unitary board concerns. Further, attitudes towards a newly formalised approach by regulators to assess the effectiveness of NEDs – the so-called 'evidence of challenge' – are discussed.

5.4.3.a. Support and information sharing

Some interviewees leaned towards a positive view of the extended regulatory presence, focusing on the ability of regulators to provide an external and potentially useful perspective on the firm, which should allow the NEDs to carry out their role more effectively. Indeed, regulators have visibility of the strategies, governance and management practices of a number of firms, and should be able therefore, in principle, to compare, contrast and identify good practice. One respondent in particular saw this as a strong positive:

> "They're a great source of information. And fundamentally, you are on the same side as the regulator" (Interviewee_06, 2014).

The same respondent also saw value in the more active approach now taken by regulators in the UK, and explained that this approach helps both communication and discussion between the NEDs and regulators:

> "The regulators have got more assertive which I think is a good thing. […] Because they should have the courage of their convictions and they should be willing to have a discussion with you […] they should be willing to say this is what we think" (Interviewee_06, 2014).

Another view was to emphasise the way in which regulators are now using NEDs as a means to achieve their own objectives. Regulatory objectives are not necessarily always the same as those of the Board and shareholders, since regulators' objectives, and their categorisation of risks to those objectives, are more naturally concerned with consumer protection and financial stability rather than with shareholder value – which is by definition the main concern of individual boards, and especially of the executive members who are incentivised to deliver profit and share price appreciation.

5.4.3.b. Confrontation and Unitary Board concerns

Others were more concerned by the effects and implications of a closer engagement with regulators on both their traditional accountability relationships and on the nature of interactions on the Board between executives and non-executives. To demonstrate this point, one interviewee thought that the quasi-reporting line to regulators increased the ambiguity of their role and indeed created suspicion between the two categories of director, which might lead to the disintegration of the unitary board:

> "And then it's inevitable that you feel you have a sort of kind of duty to the regulator as well because you're almost like a mini regulator inside the organisation and yet you're kind of a colleague of the execs, so you're sort of in and out as it were" (Interviewee_02, 2014).

In fact, this particular interviewee went further, arguing that a direct link between NEDs and regulators could be fatal to the traditional unitary board model operated in the UK:

> "It's like putting a nail into the unitary board idea. So the non-execs, if they had more contact with the regulators they'd be increasingly perceived as part of that world by the execs. And that would be not good for kind of board unity" (Interviewee_02, 2014).

In the last five years, regulators have moved from a "fit and proper test" for NEDs (which involved checking whether there is any negative reason related to past conduct not to accept an individual's appointment) to a "competence test" (i.e. formulating a question along the lines of: is this individual competent to perform the particular role expected of him or her on the Board?).

> "The regulators […] interview you and ask you questions about the detail of the business which in the past the chair of a risk committee or a board member would not have been expected to make" (Interviewee_12, 2014).

Another interviewee expressed a perception of an increasingly confrontational nature in the relationship between regulators and NEDs and, to demonstrate, mentioned the fit and proper and competence tests, which apply most explicitly on appointment but also influence the questioning of NEDs as part of their routine interaction with the regulators. This was seen as a negative sign in one case – and one generating suspicion:

> "The regulators have definitely moved from trusting you to the not trusting you. They're much more judgmental about individuals. They're requiring much higher levels of technical, financial competence" (Interviewee_03, 2014).

The most frequently expressed concern relates to the way in which this new "reporting line" affects interactions between executives and non-executives within the unitary board framework. A regular line of questioning from regulators to NEDs now includes NEDs being requested to provide evidence of the Risk Committee having a direct impact on the business though effective control systems. While NEDs accept that it should be possible to show that they have performed a useful function, regulators tend to seek examples of differences of view between the NEDs and the executive as proof that the control system is working. This in turn tends to emphasise the distance between the two groups, which is uncomfortable in a unitary board framework, and also risks changing the dynamics of the role:

> "But there's a slight tendency for the regulators to pit the executives and the non-executives almost against each other. So it's as though you're sitting on opposite sides of the table. And I think that's an unhealthy thing" (Interviewee_04, 2014).

The new and sharper focus on the nexus between regulators and individual NEDs has cut across the concept of the unitary board and the doctrine of collective responsibility. Boards are struggling towards a resolution of this conflict, in the absence of clear guidance from the regulators.

In the summer of 2015, recognising this guidance gap, the PRA organised a day-long seminar with NEDs built around a series of case studies designed to highlight uncertainties and disagreements about the role and responsibilities of NEDs generally, and Risk Committees specifically. Prior to this seminar, Chairs of Risk and Audit Committees and some other NEDs of major financial institutions received a multiple choice exam-style questionnaire with examples of case studies to be discussed. The cases were drawn from real-life examples of control failures and invited directors to assess degrees of responsibility in each case, as between the Chairman of the Board, the Chairs of Board Committees, and the executives. The regulators subsequently gave their view. This elaborate exercise is intended to lead in due course to the issuance of clearer regulatory guidance.

5.4.3.c. Evidence of challenge

A particular type of question, which appears to be common currency in financial firms today, involves the regulator asking for examples of circumstances in which the NEDs may have 'challenged' the views of Executives and either rejected or significantly altered those views. This so-called "evidence of challenge" is observed by the regulators through the minutes of board meetings as well as by sitting in on meetings and observing NEDs, and is done in a further attempt to resolve the agency problem between the regulators and NEDs. In some cases they have required skilled persons reviews (under Section 166 of the FSMA 2000) specifically focused on examining the effectiveness of risk management and board oversight. Those reviews involve extensive interactions between the reviewers and NEDs, under the guidance of either the Prudential Regulation Authority or the Financial Conduct Authority.

Due to the fact that what happens within the boardroom produces limited audit trails, and estimating boards' effectiveness can be seen as an example of "black

boxing" (Gendron & Bédard, 2006), regulators in the UK have introduced a requirement for boards to demonstrate "evidence of challenge" via "minutes and sitting in and observing Board and Committee meetings" (Deloitte, 2013b). Board minutes, however, do not necessarily provide evidence of challenge. While practice varies, and according to my observations within the firms as well as conversations with people on both types of boards, board minutes are more descriptive in the UK than in the US, even in the UK the minutes often do not incorporate difference of particular opinions discussed, as the primary function of the minutes within the firm is to provide clear direction to the executives by highlighting clear conclusions, rather than differences of view.

According to the interviewees, regulatory interviews are now therefore peppered with the language of challenge, because regulators see this as an easy proof of NED effectiveness or otherwise; while the NEDs themselves, however, tend to see this as the reflection of a misunderstanding on the regulators' part regarding the way in which a Board and its committees function:

> "The moment you make an outcome into a target you get some perverse effects. So what that has led to people being very concerned about questions they asked in board meetings that are actually minuted. I can perfectly understand where they're coming from, boards should be very challenging and therefore they want evidence of it. But the very evidence process is something which can distort phenomenon" (Interviewee_02, 2014).

Another interviewee was even more forthright and linked evidence of challenge as envisaged by regulators to failure:

> "The problem is that the regulators equate challenge as being a row. And actually that's rubbish: if you get to having a stand-up row in the boardroom you've failed, almost certainly" (Interviewee_06, 2014).

A third interviewee explained why the questioning reflected a poor understanding of the dynamics of coexisting within a collective governance framework. Indeed, it was evident from the interviews that demonstration of the evidence of challenge as an indicator of success was considered a deeply simplistic interpretation of the dynamics between NEDs and management, because it suggest

that management propose things unplanned and it is up to NEDs to reject them. In practice, however, a lot of negotiation happens outside these meetings. According to Interviewee 4, if that is how the problems were resolved it would not be a board that she would consider to be mature:

> "[FSA] once they asked me in an interview, 'How often do you turn back the proposal from the management and ask them to go away and redo it?' And I said 'Well I would regard that as a failure, that's not how boards should work. I shouldn't be sitting one side of the table and the executive sitting the other and interviewing the management and receiving a paper by surprise and saying well you know, this isn't good enough, go away and redo it. That's not the way mature, adult stuff happens'" (Interviewee_04, 2014).

This quote also demonstrates the earlier point that CRO and Risk Chair typically say they talk frequently formally and informally outside of the Risk Committee, therefore the challenge comes in those interactions rather than minuted in Board or Committee meetings.

While a fourth respondent took a more nuanced view, accepting the fact that although it is not entirely unreasonable for the regulators to look for evidence of challenge, cultural factors made this more problematic in the UK context than elsewhere, perhaps given the polite and consensual way in which Board meetings are conducted. The question of whether this was a better or worse way of reaching tough decisions was left open:

> "You can easily write notes full of meetings full of biff-baff. What do they mean by challenge? Having a big row with somebody is not helpful, it's not constructive, it's not going to get their confidence in you. […] Challenge is really asking somebody the one question they hadn't thought about and doing it in a way that they then go away and think about it and come back with something constructive. There's also a stylistic thing, there's a cultural thing as well; I mean we have incredibly forthright conversations in [another country] that I really don't think you would have in a UK board, it's just the culture there" (Interviewee_08, 2014).

Not every NED agreed with the idea of evidence of challenge as perceived by the regulators, but NEDs do acknowledge that regulators are right to require the

boards to be challenging, because, as anecdotal evidence by a chair of a risk committee in an insurance firm suggests:

> "A lot of boards and board chairmen still don't really want people on their boards who are going to be challenging. I mean they really don't. On two of the boards I was hired on, the chairman said 'I'm hiring you despite that I've been told you're very challenging' (Interviewee_08, 2014).

While, at the same time, another interviewee also observed that evidence of challenge is not a perfect tool and trust is, ultimately, at the core of the relationship:

> "I don't think you've got much alternative than to trust that the non-execs who were appointed [have] very independent personalities and will challenge" (Interviewee_02, 2014).

To conclude, while it is evident that regulators have affected, and, as the interviewees have indicated, to some extent disturbed the balance between NEDs and executives – and perhaps also between them and shareholders – it is not yet clear whether this will over time produce a better functioning risk oversight and management system. Based on the evidence of these interviews, it would seem that NEDs are unsure, and on balance negative, about the recent changes they have witnessed. The benefit of more engaged and diligent NEDs, conscious of their duties to regulators, may be at least partially offset by the creation of a more complicated decision making process. This is an area where further qualitative research, after the new arrangements have been in place for a few years, would be valuable.

5.4.4. ACCOUNTABILITY AMBIGUITY

Roberts et al. "suggest the merits of a focus, both theoretical and empirical, on the practical challenges that non-executives and boards face in creating and sustaining accountability" (Roberts et al., 2005) and warn that "The emphasis on

narrow, formal accountability within governance research presents an impoverished view of the different forms that accountability can take" – which was one of the reasons that the core questions asked during the interviews were related to the NEDs' sense of accountability.

This chapter suggests Accountability Ambiguity, as a term to incorporate both the role ambiguity inherent in the NED role itself and the difficulty NEDs experience when trying to describe their accountability to others. Accountability is seen as a foundation stone of modern institutions (Douglas, 1986). Roberts et al. draw attention to the "very different potentials of remote accountability to investors and face-to-face accountability within the board between executive and non-executive directors" (Roberts et al., 2005) – this was indeed indicated throughout the interviews, though unlike Roberts et al., interviewees in my sample paid particular attention to the regulators as important players in the accountability regime.

While role ambiguity can be seen as being primarily intrinsic to the people experiencing it, accountability ambiguity implies uncertainty in external power relations, and is motivated by the question of to whom one is responsible. Roberts et al explain that within the governance research tradition, accountability "has normally been used synonymously with monitoring or, in some cases, compliance. This narrow approach suggests a hierarchical view of relationships, with executives scrutinised by the non-executives who determine and decide appropriate categories of conformance", and instead they use 'accountability' with "a wider scope, and is intended to signal the potential for lateral processes of learning" (Roberts et al., 2005). When studying public administration governance, Salamon shows that accountability is a "multifaceted concept fraught with ambiguity" (Salamon, 2002). Ambiguous networks of accountability, where NEDs need more clearly to define and balance their accountability to the rest of the board, regulators, and shareholders, lead to fuzziness in the boundaries of the NED role.

Koppell describes the phenomenon of needing to be accountable to various parties "multiple accountabilities disorder" and explains that "conflicting expectations borne of disparate conceptions of accountability undermine

organizational effectiveness" (Koppell, 2005). In order to cure this "conceptual fuzziness", Koppell proposes a separation between five distinct dimensions of accountability: "transparency, liability, controllability, responsibility, and responsiveness" (Koppell, 2005). According to Huse, more simply, "accountability is about balancing various board role expectations" (Huse, 2005). Accountability is a widely-researched subject in the social sciences and according to Williams and Taylor it "is known for its complexity, context dependence, and ambiguity" (Williams & Taylor, 2013), and speak about *accountability ambiguity* in the nonprofit sector. Here, however, I use 'accountability ambiguity' to demonstrate the conflicting accountability demands that NEDs face.

At this point it is not clear whether these are transitional issues, related to the novelty of the role and structure, or, rather, fundamental tensions across a number of dimensions which point to the limitations of non-executive risk oversight and indicate a space within which the NED role is defined.

The overall conclusions from the interview findings can be summarised in the following table, in three categories of contribution: when it comes to relationships, accountability, and boundaries of the role. Each of the rows could be interpreted as a spectrum, and also as a direction of change from more traditional to the emerging aspects of the NED role within the risk oversight. Additionally, there is also a tension between the two columns and NEDs are struggling to balance this tension.

Table 5.2 rationalises somewhat beyond the review of interview findings, but is based on them. It presents an extrapolation based on other practitioner sources and conversations, and is therefore aimed to be a conceptual contribution to a discussion of the main areas of difference that the boards experience as compared to what they were like before the financial crisis. However, due to the fact that this is not a study that systematically compares evolution of the NED role across time, it is not possible to show each of these developments based on empirical evidence.

TABLE 5.2: STRANDS OF CHANGE

Category	Traditional	Emerging Struggles
Relationships		
Primary Role	Friend of management	Police/quasi-regulator
Interactions	Hierarchical, through CEO	Web of interactions
Regulators	Support, info sharing	Direct involvement/Unitary board concerns
Decision-making	Unitary Board	Two classes of directors
CRO interaction	Motivation, Encouragement	Monitoring, evaluating, challenging
Accountability		
Accountability	Main board	Regulators/shareholders directly
Shareholder responsibility	Through management	Also through regulators
Success	Group decision making	Individual expertise
Effectiveness	Process focused	Strategic decisions (e.g. risk appetite)
Boundaries		
Role Ambiguity	Broad scope	Deeper dives /customised focus
Involvement	Oversight	Active guidance/management
Board focus	Risk a shared concern	Delegated and compartmentalised
Info methods and flows	Internal/informal relationships	Formal Management Info, external validation/check
Time Commitment	Intermittent/occasional	Continuous

This research explores how actors operationalise risk oversight, with a specific focus on the boundary issues created by TLD, risk committees and other oversight mechanisms: the issues that different actors face in negotiating the boundary between and oversight and management are discussed. Chapter 5 has specifically focused on the role of the risk committee as seen by the risk committee members, and the boundary between the executive and non-executive roles. Oversight and management are set up as binary in formal prescription, while in order to operationalise it in practice, NEDs need to balance a number of struggles that were identified above.

5.5. CONCLUSION

The overall picture that emerges from the findings of Chapter 5 is one of complexity and ambiguity, specifically in relation to the ideal compared to practical implementations of risk oversight. The findings also show, however, that there are important areas of agreement – i.e. those areas where all the interviewees are broadly consistent in their responses. Oversight is not a clean, clear-cut category, and one does need to take on varying roles in order to be able to perform effectively as a NED: role ambiguity and conflict are inherent in the role. Katz and Kahn conceptualise organisations as being "roles or clusters of activities expected of individuals" (Katz & Kahn, 1978). Indeed, NEDs are balancing many potential tensions that can't be distilled into a simple framework. The nature of risk oversight is that it is very relationship-focused, and could be better characterised as a "web of governance" rather than as a traditional hierarchical representations**.** Roberts et al suggest that board effectiveness depends on the "behavioural dynamics of a board, and how the web of interpersonal and group relationships between executive and non-executives is developed in a particular company context" (Roberts et al., 2005).

Risk Committee members are uncertain about aspects of their roles e.g. accountability and success criteria - talking variously of being responsible to the rest of the Board, shareholders and regulators. This might be exacerbated by the comparative lack of guidance on what a Risk Committee should do, as compared to an Audit or Remuneration Committee.

Interviewees were broadly consistent in maintaining that NEDs should stay at the level of oversight and not involve themselves in management, except to change management when they are dissatisfied with management's work. They were also consistent that in spite of being removed from decision-making, non-executive oversight can nonetheless add value. Thirdly, they all see themselves, at least to a certain extent, as proxies for external regulators, focused on compliance with

regulatory requirements. The final area of agreement is their acknowledgement that, regardless of formal reporting lines, close personal relationships with key staff are still essential, in order to allow the free flow of information that enables NEDs to make a balanced assessment of the effectiveness of risk management in the business.

There are also other areas where their views diverge, and where the definition of the NEDs' role is still not clearly stabilised, with considerable uncertainty about the eventual outcome. The PRA's case study exercise, when different NEDs (and regulators) gave various arguments to questions about their responsibilities, confirmed that uncertainty while seeking to resolve it. Out of all these areas of disagreement, the nature of accountability is the most vivid example: while some NEDs see the risk committee as nothing more than a special group within the Board, which reports to the Board alone, others are however more conscious of their direct links with regulators and, in some cases, with investors. As this shows, consensus on the accountability framework is most definitely lacking.

Another area of uncertainty relates to indicators of effectiveness, especially in the absence of external sources of information as well as of external measures of success. NEDs are uncertain about how to measure their success, and some of them fear that an excessive focus on process may cause them to lose sight of the big strategic questions which, according to their view, should remain the Board's main focus.

The next chapter shows how the central problem of boundary definition between oversight and management is played out in different areas within the businesses themselves - e.g. how involved the central risk management line should get with the activities of the first line.

Board Risk committees and how they work is now the central issue in risk oversight in financial firms. That is why I spent a lot of time interviewing NEDs to discover:

- whether they are aware of the crucial role they play
- whether they believe it is possible to deliver on the regulators' expectations, and therefore
- whether it is reasonable to place heavy reliance on this oversight mechanism.

The conclusions are that NEDs are part-time and often not experts in risk management, but have been treated as a core control mechanism. They are uncomfortable with the new role definition and are struggling to meet it: indeed, there is confusion about their responsibilities and accountability and they see the new regulatory focus as cutting across the role of the unitary board. Information is easy to talk about conceptually but harder to operationalise, which is discussed in more depth in Chapter 7. It was also made clear that they see their effectiveness as heavily depending on personal relationships, which is not captured in the models of how oversight works. In particular, they depend very heavily on being given timely and accurate information. Yet that information comes almost exclusively from within the firm, and therefore information intermediaries, who process that information, play a crucial role. The following chapter discusses risk management functions within the firm, and the last empirical chapter after that looks at the information flows involved in the interaction between NEDs and the risk governance within the firms.

CHAPTER 6: RISK OVERSIGHT IN MANAGEMENT

6.1. THE THREE LINES OF DEFENCE (TLD)

Both risk governance and internal risk management systems within the firms themselves are widely perceived to have failed in the years leading up to the global financial crisis in 2007 (UK_Parliament, 2013). This chapter follows the discussion of the board risk committees because boards need the systems within the firms in order to empower them to perform their role. It uses document analysis of regulatory and consultancy documents, as well as interviews and field observations in order to understand the nature of the risk management and risk oversight systems within firms: *how is risk oversight operationalised at the organisational level in financial institutions*?

To answer that question, the specific focus of this chapter is on the Three Lines of Defence (TLD) model, which is treated by both regulators and consultants as "an embedded feature of a corporate governance framework" (FOO, 2012). As throughout the rest of the thesis, agency is used as an underlying perspective to understand the relationships that emerge when the TLD is implemented in practice.

The exact numbers for the whole financial services industry are difficult to compile, but according to EY's risk survey of asset management firms in 2012: "83% of firms have already formalized their three lines of defence" (Ernst&Young, 2012), and according to KPMG, "the vast majority of UK financial services firms employ the traditional[22] '3-Lines of Defence' model, with clear demarcations between each line in the management of risk" (KPMG, 2012). An annual report by

[22] It is noteworthy that in 2012 KPMG speaks about the 'traditional' TLD model, without giving an explanation of when it became a tradition or entered the lexicon. This is demonstrative of the way it has been used by many consultancies over time.

PwC observed that "A governance structure based on a "three lines of defense" model is emerging as a leading practice in the [insurance] industry" (PwC, 2013), and according to the 2015 EY CRO survey, 74% of insurance institutions have formally adopted the Three Lines of Defence model (EY, 2015).

As a visual representation of the idealised Three Lines of Defence model, Table 6.1 demonstrates the three lines of defence as defined by the Basel Committee on Banking Supervision's report under the title "The internal audit function in banks", published in June 2012. According to this report, the first line of defence is risk management within the Front Office, which is the primary source of income in banks; the second line of defence includes support functions, such as Compliance, Legal, Human Resources, and Risk Management and the third line of defence is Internal Audit, which focuses on the observation and evaluation of the effectiveness of Risk Management as well as other conduct within the business.

TABLE 6.1: THREE LINES OF DEFENCE EXAMPLES AND APPROACH

Line of defence	Examples	Approach
First line	Front Office, any client-facing activity	Transaction-based, ongoing
Second line	Risk Management, Compliance, Legal, Human Resources, Finance, Operations, and Technology	Risk-based, ongoing or periodic
Third line	Internal Audit	Risk-based, periodic

Source: (Bank for International Settlements, 2012)

Both risk management and internal audit are performing an oversight role over the first line. However, a clear separation between risk management and internal audit has crystallised in recent years – nowadays, as is shown below, and despite some disagreement on precisely which functions go into which line of defence, there is unanimous agreement across firms that risk management and internal audit must remain separate from each other and belong respectively to the second and the third lines of defence in the TLD model.

The board of directors, including the audit and risk committees of the board, is not a defence line by itself, but a part of the reporting structure, which is usually mentioned in the charts describing the organisation of the business: second line reports into the board risk committee and third to the audit committee. The supervision of risk internal to the business areas, conducted within these fields, is what came to be known as "the first line of defence", while the other two lines are normally found in an explicitly separate, independent risk management function at corporate or group level and in the internal audit department, respectively.

Early descriptions of the Risk Management framework for banks, articulated by the Basel Committee on Banking Supervision, considered risk management and audit together: e.g. its 1999 "Enhancing Corporate Governance for Banking Organisations", in discussion of oversight argues that "there are four important forms of oversight that should be included in the organisational structure of any bank in order to ensure the appropriate checks and balances: (1) oversight by the board of directors or supervisory board; (2) oversight by individuals not involved in the day-to-day running of the various business areas; (3) direct line supervision of different business areas; and (4) independent risk management and audit functions" (Bank for International Settlements, 1999); which, although not an explicit reference to the three lines of defence model, is very similar to the TLD approach.

As nowadays the Three Lines of Defence is "widely used within firms" (Bank of England, 2015), it is often taken for granted, as is evidenced by e.g. the most recent Financial Stability Report published by the Bank of England in July 2015 stating as one of the root causes of misconduct in the financial markets: "Systems of internal governance and control that placed greater reliance on second and third lines of defence than on trading or desk heads". Indeed, this report assumes common understanding about the meaning of second and third lines, and is also treating them as an organisational fact.

In order to understand how the TLD fits into the hierarchy of oversight within the financial institutions, this chapter first investigates its origins and emergence in regulation. It then demonstrates the variety of ways different practitioners

understand it. Finally, the chapter looks at the practical operational challenges involved in its implementation.

6.1.1. HISTORY

The TLD language was used in all organisations I have observed or otherwise interacted with throughout this research. The Chief Risk Officer of Aviva Europe, a major insurance firm, wrote: "It needs to be stressed that risk management is not only carried out by the risk management function, but by the whole organisation. The organisation can be split into the so called three lines of defence" (Koller, 2011).

Historically, although there is no consensus on how the three lines of defence concept entered the risk domain, there are some sources (Bonisch, 2013) which observe that it might have originated from either the military or from the field of sports. Search results obtained on Google Scholar[23] included studies from journals as diverse as Parasitology, Veterinary Studies, and Petroleum Engineering, while the entries about risk management focused primarily on operational risk. When using the American English spelling of the word (defense instead of defence), the search[24] resulted in entries from journals on Nutrition, Medicine, and Terrorism. On Google, the search outputs prior to 2003 were primarily about immunology and warfare. There are also defence lines in American football and basketball (though not normally three), but it is unclear how the idea transferred into the language and practice of corporate governance and risk management.

---

[23] Scholar.google.co.uk Exact search term: "3 lines of defence". Date: June 5, 2013. 14:16GMT

[24] Scholar.google.co.uk Exact search term: "3 lines of defense". Date: June 5, 2013. 14:52GMT

The first reference related specifically to the financial sector that I identified is by Roman Kräussl, from the Center for Financial Studies at the Johann Wolfgang Goethe-Universität Frankfurt in 2003, who speaks about the "lines of defense against systemic risk in international financial markets", by this meaning "market discipline, prudential supervision and regulation, and macro-prudential surveillance" (Kräussl, 2003). The focus of this thesis, however, lies on the more recent use of the three lines of defence model *within* organisations, rather than a part of regulatory landscape. The following section examines the emergence of the firm-level TLD concept within the UK regulation.

6.1.2. EMERGENCE IN REGULATION

The first reference to the 'Three Lines of Defence' in the FSA's publicly available documents dates from 2003: "A number of firms had adopted a 'three lines of defence' approach, where business line management provided the first line, risk functions the second line, and internal audit a third line (each of which reported into different executive management)" (FSA, 2003). It would appear from this statement that firms had adopted the three lines of defence model without the FSA requiring them to, though it is not clear what the driver for this adoption was. And while according to some consultants (Burden, 2008) the FSA required firms to take the three lines of defence approach to risk management in their 2003 ARROW (Advanced risk responsive operating framework) review, I was not able to observe this practice or confirm it from the documentation (FRC, 2010a).

One Chairman of a risk committee in a major financial institution confirmed during the interview that the TLD terminology emerged quite late in the day to day vocabulary of risk management in banks:

> "I didn't actually hear much about it until 2007 or 2008. At that point I'd been in banking for 12/13 years and I don't even remember it being said" (Interviewee_07, 2014)

In the UK, the codes of practice in the corporate governance area have been articulated by a series of reviews commissioned by the Bank of England, HM Treasury and other bodies; their reviews typically have received significant input from the practitioners during their production and they are implemented on a "comply or explain" basis. So risk management is covered by a complex mixture of black letter regulatory requirements and softer, practitioner-driven guidance embedded in codes of practice, sometimes 'adopted' by regulators as appendices to their rulebooks. Chapter 3 covered different regulatory practices in more depth. It is important to point out that the two most relevant events regarding the three lines of defence framework were the Cadbury review which in this context focused on audit committees, and the Walker review (Walker, 2009), which institutionalised board risk committees.

The Cadbury review, discussed in Chapter 4, does not mention the "three lines of defence" model explicitly, but some of the points discussed are fundamental to three lines of defence. Specifically, Cadbury suggested division of responsibilities, such that no one individual has complete powers of decision, and at least three independent Non-Executive directors should be present on the audit committee in order to oversee the financial reporting. This narrative of separation of responsibilities and independence of oversight has a strong resemblance to the way TLD is spoken about. The Walker review of Corporate Governance also does not contain an explicit reference to the TLD, but it takes audit committees for granted and explains why risk committees are necessary, thus assuming the third line as being in place and suggesting board-level oversight of the separate second line.

6.1.3. POST - CRISIS

As was demonstrated in Chapter 4, in 2010, as a consequence of the global financial crisis and the Walker review, the UK financial regulator became far more interested in risk within the businesses themselves and with the way these risks are managed internally. The FSA no longer limited itself to external oversight of prudential soundness and business conduct, but instead became increasingly involved in the way firms should organise risk oversight internally. While the Three Lines of Defence framework has been institutionalised into a common practice in most financial institutions in the UK, it is unclear whether this is a mere repackaging of the structures which had been in place before or is indeed a significant alteration of the substance of risk management practice – one might argue incorporates elements of both, but further is needed to confirm that hypothesis.

The FSA's consultation paper on "Effective corporate governance: Significant influence controlled functions and the Walker review" published in 2010 included the first mention of the term "Risk Oversight" identified in any publicly available documents. The FSA also stated, in the same paper, that "we have long stressed the importance to regulated firms of an effective and independent risk oversight function ('second line of defence')" (FSA, 2010b). So, here, the FSA treated the independent risk oversight function as something which had always been required and which had been discussed before; additionally, the wording of this sentence implies that risk oversight is also something that has always been done, but I have not found any evidence of earlier mentions in their publicly available documents. The sudden emergence of the Three Lines of Defence framework could be seen as symptomatic of the increased emphasis of the regulatory focus on risks within firms which was tracked in Chapter 4.

The impact of these new regulatory requirements, particularly the increased role of the risk function, as recommended by Walker, was very evident at the firm where I conducted a participant observation in 2012 – i.e. the role of the CRO had indeed changed after the financial crisis and now he reports directly both to the CEO and Chairman of the Board (the same person in the US context). There now also is an added parallel reporting line to the Risk Committee, who must also be consulted on the CRO's remuneration, while previously, the CRO only reported to a business head. This demonstrates that the role of the CRO and the risk committee has become more important and the risk profile became a starting point for discussion instead of looking at transactions purely in terms of expected returns.

Non-executive directors now generally accept that TLD is the standard structure for the effective risk management framework, one risk committee chair characterised it as "as good a model as any to be honest and probably the least worst" (Interviewee_05, 2014). Another described it as a "well-tested model for risk management and control" (Interviewee_07, 2014). But they are not uncritical. One suggested that the model could downplay the importance of strong risk management in the business areas themselves: "not enough emphasis is placed on the first line of defence which is management […] the first line of defence is the most important line" (Interviewee_07, 2014). Another underlined the point more firmly "my problem with it is when fundamentally the responsibility for the risk gets taken away from the business because ultimately it's the business that manages the risk. […] the three lines of defence is useful but cannot take away the responsibility and accountability from the firm" (Interviewee_06, 2014).

A related concern is that TLD might result in an excessively bureaucratic, costly, and demotivating approach to risk management. One interviewee suggested that:

> "You can be quite good at managing your business, your risk, your strategy, but the other key part is about doing it efficiently. You could have a very well controlled business by having somebody sitting next to everyone checking everything that they do. Everything front to back from the minute a client's account is opened or an order is taken, you could have a risk person or a compliance or an audit person shadowing everything; that would be kind of

safe. It would also be kind of expensive and not a very nice place to work probably" (Interviewee_07, 2014).

This explanation clearly demonstrates that while adding layers of oversight might make the processes safer, firms have to be cautious to do so without getting into unreasonable detail as Interviewee 7 explained. The request to add more oversight whenever things go wrong is an easy one to make, but questions about efficiency remain to be answered.

Additionally, despite being universally accepted as something that is done, and also appearing so clear, with each line being separate and distinct in writing, there is still some significant disagreement about particular aspects of the model, and considerable divergence in the manner of its operationalisation within firms. The regulators' and consultants' theories must be translated into the reality of oversight and management from day to day: that can be a messy process, as the following section demonstrates.

6.2. AMBIGUITY IN DEFINITIONS

Since in the spirit of its principles-based regulation, the FSA did not offer an explicit explanation about how the three lines of defence model could be introduced into organisational practice, as a result there are a number of different representations created by consultants of what the idea of the three lines of defence might look like in reality.

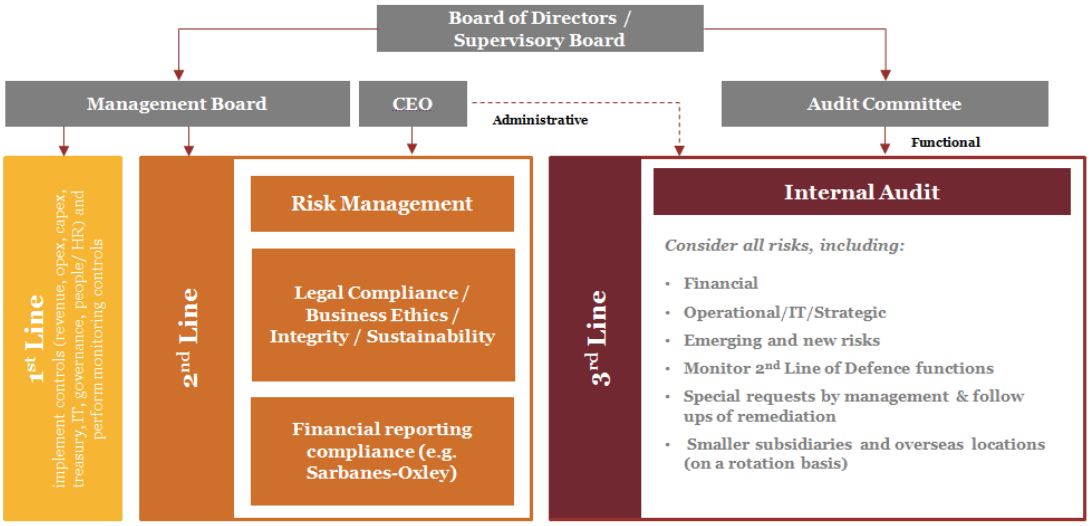
Three Lines of Defence in practice, while it is common use, has varying interpretations. Below is a sample of four different representations by the major audit firms of the three lines of defence model. As a side note, these representations are not typical of every existing consultancy report and they are shown to illustrate the range of models described rather than to attempt providing an elaborate understanding of what the variation is like.

The depictions by PricewaterhouseCoopers, KMPG, Deloitte and EY were chosen, as these are the so-called "Big 4" audit firms, which advise the major financial institutions like those where field immersions and interviews were conducted. They each give prominence to the internal audit function in their models, which is perhaps not surprising given the source.

While a common pattern amongst all these representations is the fact that each line is separate and distinct from the others, in practice when analysing organisational charts it became evident that these separations might be much more difficult to achieve due to the complexity of the organisation and also to the fact that people might have overlapping roles or might have to work together in the long-term and might, as a result, have different incentives. Therefore, the TLD model provides an idealised view of how these functions should interact with each other and with management above them.

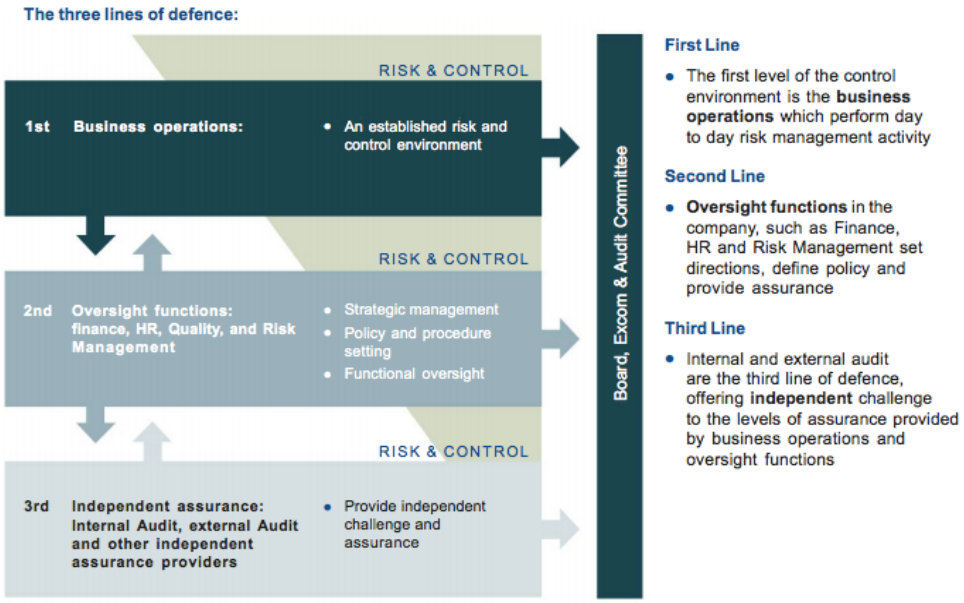
One interviewee, a Risk Committee chair, while regarding TLD as "absolutely appropriate" in theory, drew attention to the practical complexity of determining appropriate reporting lines: "they should have clear and independent reporting lines […] you should separate the three lines at the highest level [but] one of the biggest problems I've seen is actually a second line of defence that is not separate from the business […] and it's not separate far enough up. […] think risk and control functions should be independent as far up the chain as they can" (Interviewee_07, 2014).

FIGURE 6.1: PWC TLD FRAMEWORK



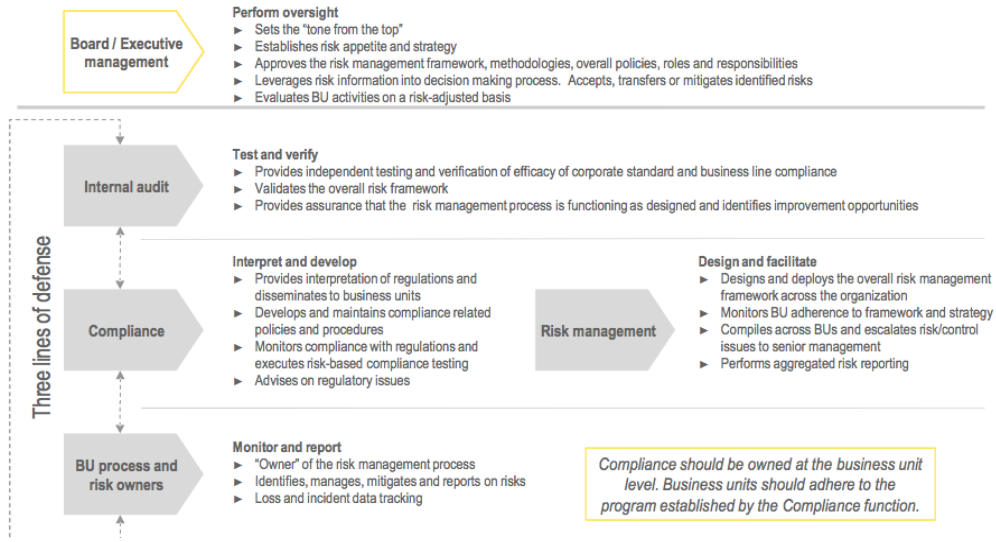
Source: "Effective Internal Audit" (Pwc, 2015)

FIGURE 6.2: KPMG TLD FRAMEWORK



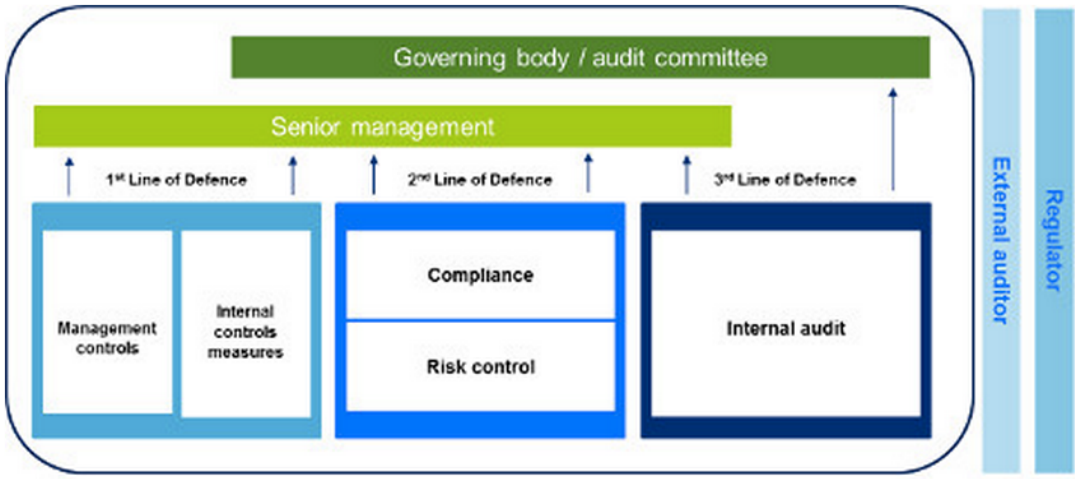
Source: "The Three Lines of Defence" (KPMG, 2013b)

FIGURE 6.3: EY TLD FRAMEWORK



Source: "The Three Lines of Defense in Effective Risk Management and Control" (EY, 2013b)

FIGURE 6.4: DELOITTE TLD FRAMEWORK



Source: "Internal Audit in Financial Services" (Deloitte, 2013a)

The table below provides a summary of the exhibits above from the Big Four:

TABLE 6.2: SUMMARY OF BIG FOUR REPRESENTATIONS

	1st line	2nd line	3rd line
PwC	Controls: IT, HR	Risk Management/Compliance	Internal Audit
KMPG	Business Operations	Oversight Functions, HR	Internal & External Audit
EY	BU Processes	Compliance/RM	Internal Audit
Deloitte	Management Controls/Internal Controls	Compliance/Risk Control	Internal Audit

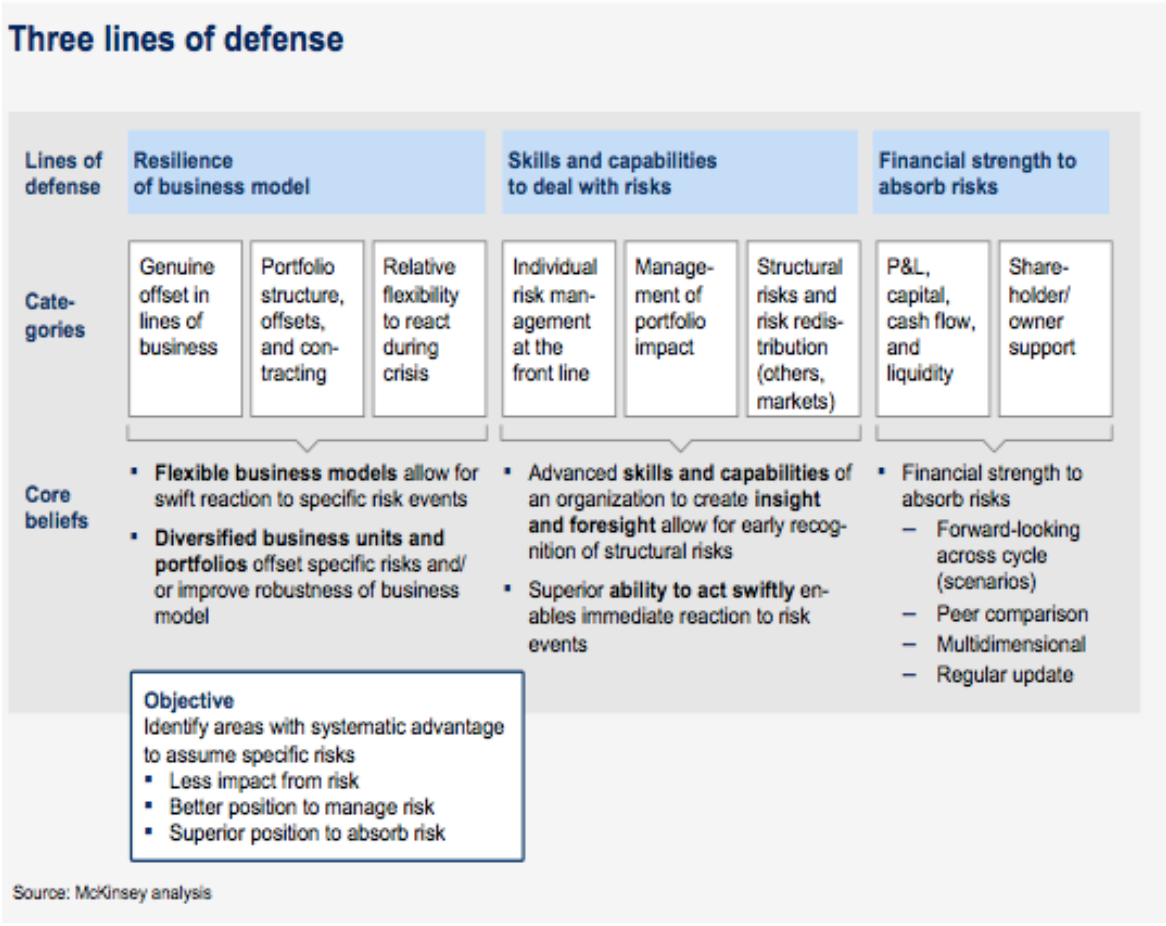
Although the first line includes the business units in all cases, PwC also include Information Technology, governance, and Human Resources (HR); and although the second line always includes risk management and compliance, KPMG adds HR to the second line. The fact that KPMG is the only one of the four that places HR above the business unit risk management is surprising, since risk culture stems from the people hired and, thus, HR plays a crucial role. However as HR is not involved in direct business decisions regarding transactions and limits, it would also make sense not to include it into the framework.

McKinsey's definition is completely epistemologically different in "Getting risk ownership right" is demonstrated in Figure 6.5 – since Mckinsey is a leading management consultancy, it could be seen as surprising that their conceptualisation deliberately diverges so much from those of the Big 4. It emphasises the qualities needed in a firm to ensure satisfactory risk oversight and management, rather than the organisational structures and checks and balances between the lines. This might suggest that TLD is heavily driven by the idealised work of auditing (and risk

management) professions, potentially attempting to define and give themselves a role.

The standard definitions of TLD as those by the big 4 suggest separate processes working in sequence, with each following line capturing any issues that might have been missed by the previous one. In case of McKinsey's representation the sequence is not obvious, and TLD is conceived not as organisational layers of oversight, but rather as a way of slicing business into the range of activities within the firm, based on how macro-or micro they are: with "categories" ranging from individual, to business unit, to portfolio – level.

FIGURE 6.5: THREE LINES OF DEFENCE ACCORDING TO MCKINSEY



Source: Getting risk ownership right (McKinsey, 2010)

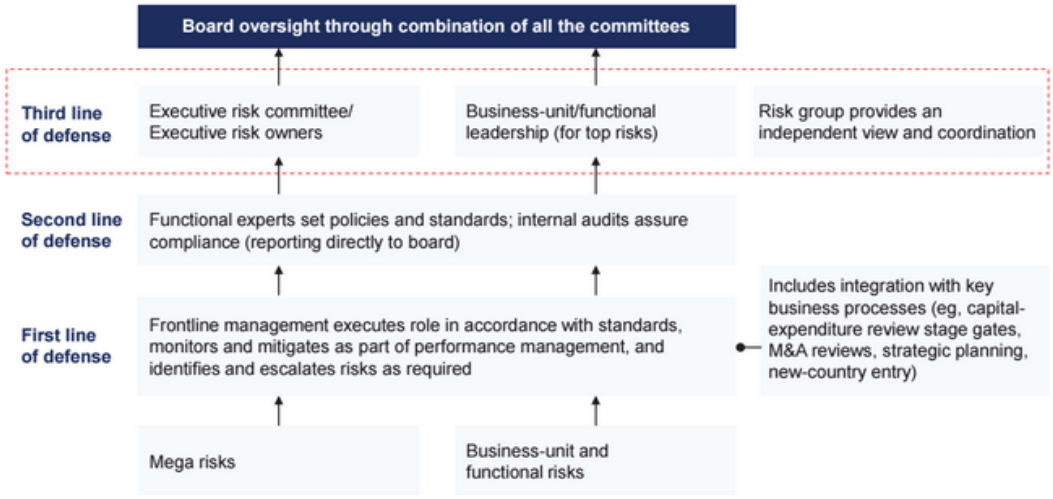
In 2012, however, in a paper on "Enterprise risk management: What's different in the corporate world and why", McKinsey defined TLD as

> "A common framework for risk management, especially in the financial sector, is that of "three lines of defense," the first being line management/front office, the second the risk- management function (and/or other control functions), and the third compliance and audit. This framework is typically brought out to emphasize that the risk-management function does not operate in isolation, and that robust risk management requires all three defensive lines to be in place" (McKinsey, 2012).

This definition is, except for the role of compliance, entirely in line with those by the Big 4.

In 2014, as demonstrated in Figure 6.6, McKinsey presented a more conventional view of the lines of defence, though it still varies from those by the Big 4, and includes a separation by the scope of risk.

FIGURE 6.6: THREE LINES OF DEFENCE ACCORDING TO MCKINSEY IN 2014



Source: "Enterprise-risk-management practices: Where's the evidence?" (McKinsey, 2014)

McKinsey mentions risk committees in the third line, and audit and compliance in the second line. Based on observations during the field research, compliance might also belong to the first line, since these people support both the first and the second lines, and the distinction between the two is blurred. The main blurring, however, could be attributed not to whether a given activity belongs to the first or second line, but the inconsistent use of the term "Compliance" and the activities it encompasses. At its widest, it is used to cover the scrutiny of a new client instruction form for confirmation that it meets the relevant conduct requirements (anti-money laundering, best advice, treating customers fairly, understanding customer needs etc.) Such scrutiny could be in the form of taking random samples or be part of the process prior to the instruction going live. The intermediary may refer to the proposal needing to go through the company's compliance team before being issued – in practice this is always a first line activity; unless the Sweeting "offence and defence" model is militantly followed (see more on this model below).

At the other end of the spectrum, a business may have a head of Compliance and Regulation (or a similar title) – a second line role that will oversee the formation and effectiveness of compliance policy and articulate the appetite for compliance risk. This person and their team will ensure that the two functions described above exist and are effective as well as requiring material breaches to be escalated for inclusion in management information within a risk report.

According to a senior manager in a risk division of an insurance firm, while HR is in charge of remuneration, which thus in theory gives them control over risk behaviour and incentives, in fact HR people do not have the power to change risk-taking behaviour in more direct ways, whereas line management of each division is more important in determining remuneration structures. HR, however, can have an impact on the way TLD becomes crystallised within the organisational setting by changing the ways employees within different lines are remunerated. To demonstrate, in one institution I observed, the 1st and 2nd line staff received annual bonuses which were split into a component based on personal performance and a component based on corporate performance (the latter being a stated formula based

on the key financial metrics for the calendar year, a simplified version of the Total Shareholder Return metrics that typically underpin the vesting of executive share options). While the actual split varied by grade, 50/50 was not uncommon. The third line staff however did not have a corporate performance bonus component; their entire bonus was based on personal performance. According to a conversation with a senior director in that firm, the rationale was that internal auditors should not feel conflicted if they had cause to unearth a serious audit issue that would lead to a hit to published results and hence a lower bonus.

When a new Group CRO was appointed in that institution, briefly before the period of my observation, he together with HR decided that the 2nd line was also exposed to such a conflict and were therefore moved to a 100% personal performance bonus structure. A senior interviewee within that firm explained that in his opinion: "I saw this as an unhelpful portrayal of the role of risk: risk should help the company generate better decisions, meaning ones that suitably reflect the risk-reward trade-off. So I saw it as entirely consistent that by challenging a 1st line proposal, I was helping achieve a better overall corporate return on capital which should feed into our results" (Insurance_5, 2013).

This example demonstrated that the TLD model had provided a structure whereby the mix of personal and corporate bonus could be set separately for each of the three lines, and therefore the line definitions were reinforced by the theoretical construct of an organisational model.

However, all of these definitions have a point in common, which is that internal audit belongs to the third line. Taking into consideration that these are the big 4 audit firms, it is not surprising that the third line – internal audit – is given a relatively significant proportion of each representation and indeed is represented as having higher weight than the other lines by e.g. PwC and Deloitte. KPMG also adds external audit and other independent assurance providers to this third line, which might be an indication of functionality (internal and external audit typically do some work together or at least co-ordinate their work programmes), rather than of the hierarchical positioning as External Audit is outside the firm.

Despite not being internal to the firm's organisation, external audit is also often mentioned as a part of the firm's corporate defence. External audit provides a separate independent assurance, and is "critical to protecting a financial institution and provide a basis for corporate boards to ensure that asset valuations and accounting are correct. Indeed, the failures of financial firms are closely intertwined with lapses in the oversight of their external auditors" (Ludwig, 2012). However despite its criticality, external audit is not a part of the TLD. Internal audit is independent of business unit management, or should be, but remains paid and employed directly by the firm (except in the case of very small firms which are outside the scope of this research).

In July 2013, the Chartered Institute of Internal Auditors issued a set of recommendations entitled "Effective Internal Audit in the Financial Services Sector". One of the things this guidance explains about the role of Internal Audit is that "Internal Audit should include within its scope an assessment of the adequacy and effectiveness of the Risk management, Compliance and Finance functions" (IIA, 2013). This guidance was welcomed and endorsed (Bank of England, 2013): According to Martin Wheatley, Chief Executive of the Financial Conduct Authority from 2013 to 2015: "Internal auditors must be front and centre of ensuring their firm acts with integrity and will be alert to potential risks" (Bank of England, 2013). Regulators welcome expansion of the internal audit role because "Internal audits are used to ensure that risk management and compliance systems are working properly and that businesses are operating within the law" (Ludwig, 2012).

Protiviti, a risk management consultancy, adds to this that the "3rd line of defence is provided by the board audit committee and the internal audit function" (Protiviti, 2012). While the board audit and risk committees are also sometimes mentioned in the charts showing the way the three lines of defence work, they are typically depicted as above and separate from the three lines, not a part of them, again due to the fact that the board is not a part of the internal risk management infrastructure. This separation is due to the fact that lines of defence are seen as feeding information up to the board-level and helping the board members make informed decisions: second line into the Board Risk Committee and the third line

into the Board Audit Committee. The third line also feeds into the Board Risk Committee in matters regarding risk management, as was explained in Chapter 5. In addition to the question of how the lines are separated, the following section presents an overview of major challenges that organisations might face when implementing the three lines of defence model.

6.3. Operational Challenges of the TLD Framework

On the spectrum between management and oversight, the first line business unit risk management is closest to *management* not oversight, and the third line (internal audit) is the most pure oversight function. Based on the field observations and desk research, I assume there is no sharp distinction between these two categories, and they could be understood as belonging to the same spectrum, which assumes a level of fluidity of the concepts and their implementation.

The second line of defence – risk management – is where there is most disagreement about whether staff should be involved in risk management actively, by e.g. participating in approval of each significant transaction, or instead oversee risks in a way that is similar to internal audit. The following section presents an analysis of difficulties in operationalising the three lines of defence model and introduces the main criticisms associated with this idea. The three lines of defence could be seen as an organisational instrument to facilitate oversight within financial institutions in practice. Due to the ambiguity of particular aspects of the meaning and the lack of a universally agreed definition, one could describe three lines of defence as an "overused metaphor" (Bonisch, 2013). Strikingly, none of the conversations I had with employees in the first line had referred to themselves as 'the first line', and indeed were frequently not aware of what the metaphor means, while that language of self-identification has been unanimous in the second and third lines.

Some argue the framework does not include all the levels that it should (Lyons, 2012), e.g. while executive and non-executive directors have a part to play in oversight and information from different lines feeds into them, they are neither a separate line of defence nor are they a part of the regular three. Following this line of discourse, one could also argue that, as an example, the board risk committee, being in charge of the second line of defence, is also part of the second line, but on the other hand this argument is flawed because non-executive directors do not actively interact with the lower-level first line in the same way as the second line does, and they are indeed part of the more complicated oversight hierarchy that this thesis investigates.

The TLD model has come into greater prominence recently, but, as we have seen, it was in operation before the crisis and one might argue it did not prove itself effective in preventing or containing the crisis, though supporters argue it has been made stronger since. The UK Parliamentary Commission on Banking Standards report published in June 2013 explained that "Fashionable management school [Three Lines of Defence] theory appears to have lent undeserved credibility to some chaotic systems. Responsibilities have been blurred, accountability diluted, and officers in risk, compliance and internal audit have lacked the status to challenge front-line staff effectively" and indeed provided a "wholly misplaced sense of security" (UK_Parliament, 2013).

This sense of security was caused by the fact that there were three separate groups who were supposed to ensure proper conduct towards risks. However, this might have been more of a problem than a solution, since one could argue that when there are several people in charge – no one really is. Another way of looking at it is that having several lines of defence diffuses responsibility rather than creating a more rigorous system. It is thus not surprising that there currently is some regulatory scepticism about the three lines of defence model, but for the purpose of this research it is useful to observe that there is simultaneously a degree of public focus on the model that it did not have before. Broadly speaking, regulators and firms are attempting to strengthen TLD, rather than seeking a radically different replacement for it.

The commonly accepted failing of the TLD model during the crisis led to several additional influential responses, e.g. the publication of The Internal Audit Guidance "Effective Internal Audit in the Financial Services Sector" in July 2013 (IIA, 2013). This guidance acknowledges that "Effective Risk Management, Compliance and Finance functions are an essential part of an organisation's corporate governance structure" (IIA, 2013) – indeed the guidance was specifically designed in order to clarify and strengthen the role of the third line of defence, and it explains that internal audit needs to continue remaining independent from the other functions, and "be neither responsible for, nor part of, them" (IIA, 2013). The Internal Audit Guidance has also brought attention to the risk-based internal audit by saying that internal audit should make a "risk-based decision as to which areas within its scope should be included in the audit plan" (IIA, 2013).

In my own research, during an interview with a head of risk in a major insurance firm, he expressed scepticism about risk-based internal audit, because, he explained: risk management is a top-down activity, while internal audit is a detailed horizontal process. Their tasks complement each other in that they provide a thorough investigation by looking at issues from different angles. If audit will be required also to become top-down like risk management, the whole point of internal audit might be lost. The ambiguity in definitions discussed above might present a challenge in operationalising TLD. Several other potential practical issues in operationalising it are discussed below.

6.3.1. Three Lines of Defence in Practice

One of the reasons the three lines of defence approach was encouraged by the FSA as well as a dense network of other actors (consultants, auditors, etc) is that it gives structural content to oversight and therefore makes the process itself auditable and comparable. TLD is an easily understandable concept, but as is evident from countless consultancy attempts at explaining how TLD should be organised within

the institutions, there might be challenges in practical implementation due to the fact that that it is primarily about the structures and functions that should be in place, not the complicated information flows between them. Effectiveness of risk management strongly depends on how each of the lines interacts with the others, and that is more difficult to observe and measure than the committee structures that are in place. Sweeting observes that while TLD provides a good explanation about the division of responsibilities, "it leaves open the degree of interaction between the three different lines, in particular the first and second" (Sweeting, 2011).

6.3.2. Models of Interaction

In order to explain the variety of implementation practices, Paul Sweeting identifies three styles of risk management interaction alongside the three lines of defence model: (1) 'offence and defence', (2) 'policy and policing' and (3) 'the partnership model'.

1. The 'offence and defence' model is the textbook approach to risk management, because it explains that the first line is purely interested in maximising gains, while the second line is only focusing on minimising the risks: the "first and second lines are set up in opposition. There is no incentive for the first-line units to consider risk [...] Conversely, the [second line] has an incentive to stifle any risk taking – even though taking risk is what an organisation must often do to gain a return" (Sweeting, 2011) I did not expect to find this approach in its pure form in the organisations I observed in the financial sector, because the financial crisis emphasised the importance of risk management, and a fully profit-driven first line would not be encouraged. The 'offence and defence' model is unlikely to be rigorously followed in practice, as it is common to encourage cooperation between the lines as outlined by the following two modes of interactions.

2. The ‘policy and policing’ model involves the Risk Management function “setting risk management policies and then monitoring the extent to which those policies are complied with” (Sweeting, 2011). This makes Risk Management more of an oversight function, because it is policing whether the behaviour of the first line is in accordance with its frameworks and requirements, rather than having an active confrontation. The risk management function in the headquarters of an insurance firm I observed in 2013 was closer to this model, where setting and refining of risk policies for the businesses was a frequent conversation point. For example, the Head of Model Oversight (part of the second line risk management) when describing the role of the second line towards the first line said: “Our role is to tell them where they should improve, and when they say they note it, it is our role to decide whether we are happy that our concern was noted and minuted, or whether we want to insist that they come back with their corrected homework. And then we hope and check whether they do their next homework better” (Insurance_5, 2013). The question that arises, therefore, is not just how to implement the structure, but also what does management does with the output of the TLD. This approach may have been prevalent in that organisation due to the fact that this firm has a federal organisational structure, which means that the business units have power over their own processes, and the role of the headquarters is to oversee the risk management within the business units and ensure they have the right structures and frameworks in place.

According to a senior risk executive within the investment bank where the first participant observation was conducted: **“**Risk is not exactly the police, risk works with the business. So when a trade is not done or a business decision is taken not to go ahead with something, usually it’s the result of a maturing process. It’s not like Risk saying you can’t and the business saying ‘Yes, I can’, it doesn’t work that simplistic” (Bank_5, 2012). The ‘policy and policing’ model can be seen in operation when the firm has a clear risk appetite set at the top, with clearly articulated self-components which allow it to be used in individual business units. In a bank, for example, this might have the form of

limits on exposures in different credit risk categories (usually defined by credit ratings). In an insurance company it might be carried out as limits on particular types of business, e.g. on exposure to longevity risk. If these limits are well-defined the 2nd line of defence can then effectively police them, elevating breaches to the Board Risk Committee. These limits can be accompanied by so-called 'triggers' somewhat below the absolute limit, which allows early warnings of potential breaches.

3. The 'partnership model' involves business units and risk management "working together to maximise returns subject to an acceptable level of risk. It can be achieved by embedding risk professionals in the first-line teams and ensuring that there is a constant dialogue" (Sweeting, 2011). This was the goal of the bank I observed in 2012: their risk division was split into those who were on the trading floors with the first line, and those who were in a central risk management function separate from the first line. The risk managers separate from the first line were supposed to interact with the first line on a regular basis, and physically spend some time there (working with the first line directly, on their floor) every week. However, during the interviews most people mentioned that in practice they didn't always have the time to go there, and thus did not have as much of a constant dialogue as they would have liked. A certain level of distance is also needed for the second line in order to be able to "give an independent assessment of the risk management approaches carried out by those units" (Sweeting, 2011), without getting so involved in the everyday practice that they miss some issues and normalise the deviances.

The above three examples of how the interaction between business lines can be categorised demonstrate that there is a lot of variety within the seemingly simple three lines of defence model. It is a simple, almost too simplistic, model that makes risk functions in the otherwise complex domain of enterprise risk management appear vividly distinct: in reality, however, these lines are much more blurred, and the categories are fluid, which makes labelling interactions as one or the other less possible.

The idea that lines are complementary and are used to refine decisions rather than stop decisions from being made presents a very different way of approaching the structure than if the interaction between them means checking on/policing each other. Policing might lead to fighting for territory instead of collaborating productively. It would also be possible to argue that the third line is not really a "line of defence" in terms of protecting business from the outside world, like the first and second lines, but instead the third line is checking whether the first two are functioning according to the rules, which is principally different from providing judgment regarding the nature of the transactions themselves (not just the way they were executed).

One point that arose during several interviews is that calling the organisational structure "lines of defence" has a negative connotation, because it is not clear what the business is defending itself against. Are the lines of defence there in order to protect the business from the follies of its own management, or in order to protect it from some external danger? According to an interview with a head of model oversight in a risk management function in a large insurance firm: "the three lines of defence should be called the lines of opportunity. Each line is not trying to stop the process at each stage, but improve it instead" (Insurance_5, 2013).

Indeed, all lines could also be seen as working together towards the protection of the common risk appetite crucial to the business. Their effectiveness could therefore be conceived as depending on how clearly risk appetite is defined. That dimension is discussed further in the next chapter.

6.4. CONCLUSION

To summarise, a famous observation by George Box in the Journal of the American Statistical Association that "All models are wrong, but some are useful" (Box, 1976) is relevant here: despite its obscure origins, variation of meanings, and challenges in implementation, the Three Lines of Defence has evolved into the main method of organising risk management within firms. Despite being the main organising principle, it is not clear whether it is preferable to alternatives that were not discussed above. It can be seen as an attempt to create (hopefully constructive) challenge and tension within the firm by setting up units with different objectives, reporting lines, and methods of compensation. Ultimately it can be seen as the structure set in place to define and defend the company's risk appetite; therefore while risk appetite has been mentioned earlier, the way it happens as a *process* is discussed in the following chapter.

This Chapter began by demonstrating the unclear origins of the framework that did not prevent the TLD model to come into prominence and be widely used and accepted. The chapter then moved on to showing a selection of existing interpretations of the organisation of lines, and pointed to the fact that representations by the Big 4 accentuate the role of internal audit. Finally, the chapter explained that the TLD model expresses the idea of risk oversight, u it provides the Board with multiple approaches to risk within the firm, and allows a reassurance that risks are covered as completely as possible.

Essentially, the differences of opinion that may arise from within this multi-level risk approach could have been inconspicuous were each of the lines not required to produce explicitly separate information. This variety of opinion should in theory increase the effectiveness of Board oversight: non-executive directors are by definition external; therefore they depend on accurate information, presented as complete and multi-sided as possible in order to inform their strategic decisions.

A major caveat in TLD, however, is that despite the additional reporting lines into the board committees, all the units ultimately report to the CEO, so the independence may not be as real as it looks. Some think the system is unlikely to discipline risk-taking effectively, partly due to the blurring of reporting lines and responsibilities. It is unlikely to work well unless there is effective oversight by people who do not report to the CEO. So the fact that regulators have in addition began to place heavy reliance on the Board of Directors and especially on independent directors in the Board Risk Committee could also be seen as being connected to the TLD.

The TLD model depicts a "conceptual delineation of control levels" (ECIIA, 2012), which provides a structural solution around which the processes and information flows need to be organised in order to make it truly operational. Due to the fact that the lines are not as clear-cut as they might initially appear to be, there might be gaps in the information flows which are not covered by the model – thus TLD could also be explained as the information flow problem.

Reporting lines are problematic because it is difficult to achieve meaningful independence when all the employees are working for the same firm. Additionally, the streams of information have to be structured in such a way that there are no "dead ends" where information gets lost when it flows upstream to the level where the key messages might be lost. The overarching objective of the three lines of defence is that separate functions report on the same issues from different perspectives which ensures that the board gets as full a picture as possible about what is happening within the organisation, which is the focus of the following chapter.

CHAPTER 7: INFORMATION INTERMEDIARIES

7.1. INTRODUCTION

> "The ability of the board or a committee to perform its oversight role is, to a large extent, dependent upon the relationship and the flow of information between the directors, senior management, and the risk managers in the company" (Wachtell, 2015)

This chapter examines the way information for Board members is assembled, measured and filtered, with the process of setting risk appetite at the core of it. So far risk appetite has been examined from the perspective of theoretical definitions, but this chapter looks at the way it is operationalised in practice. Specifically, the focus is on the interaction between the board and management in this process, based on the observations and interview materials. The objective is to provide a level of detail that is often missing from general statements common in practitioner literature such as "The board of directors must establish the institution-wide Risk Appetite Framework" (FSB, 2013b).

Chapter 5 analysed how risk oversight is exercised by the Board and its Risk Committee, while Chapter 6 demonstrated that the Three Lines of Defence is currently the most commonly used organisational architecture that makes the risk management work of the Board possible. As these chapters explained, information is at the core of any oversight practice; providing it, accurately and comprehensively, is also a continuous struggle for the various parties involved. A major part of that struggle is caused by the ambiguity of the meaning of 'oversight' itself, as well as what information is needed. The chapter explores these struggles, primarily from the NED perspective, but also with help of interviews from those who provide information for Boards. This chapter is more speculative and based on

more fragmented data than the earlier chapter, and therefore hopefully demonstrates more opportunities for future research.

The Walker review of corporate governance cites defective information flows as the central cause of the failures of financial institutions: “Failures that proved to be critical for many banks related [...] to defective information flow, defective analytical tools and inability to bring insightful judgment in the interpretation of information and the impact of market events on the business model” (Walker, 2009). It is notable that Walker differentiates between information itself and the board’s ability to use that information to make relevant judgments, but he sees the provision of defective information as a key factor behind boards’ failures in the area of risk oversight.

Most interviewees acknowledged the significance of the information flows and risk appetite process, but the particular elements of it were rarely problematised. Risk appetite is a key area where the knowledge that NEDs need in order to exercise their role has to be constructed by the information intermediaries and the NEDs working together, in a continuous process.

My thesis focuses on knowledge-based, financial institutions, where information suppliers are present on many different levels throughout the firms, but the specific focus here is on information intermediaries who transform risk-related information in order for it to be used for risk oversight and strategic decisions at the board level. In the two organisations I have observed, the functions that served as central nodes of information transmission were called Portfolio Analysis, Risk Reporting, ERM, and Risk Oversight. Each of them had a slightly different domain of responsibilities, for example Portfolio Analysis was primarily preparing management information for the board level, while Risk Reporting was more focused on the flows of information within the risk function, but the unifying aspect of all four was a close reporting proximity to the CRO and the board, as well as the fact that the core of their role was processing and making information relevant.

> "So you're giving them this piece of MI[25] […], so what. That's exactly what the Board needs to know: not the data, they need information which is the data made relevant (Insurance_13, 2013).

This quote demonstrates that relevance to overseers comes from processing vast amounts of data into usable information, and the role of information intermediaries is to make that transformation with the right audience in mind.

The chapter uses the perceptions of people involved in producing, digesting, and receiving various information flows, primarily focusing on the Board, in order to investigate those flows. These processes could be seen at the core of corporate governance, which might be conceived as having the purpose of eliminating or minimising information asymmetry problems. Various management structures in the firm, including the overseeing NEDs, depend on the effectiveness of the infrastructure of systems and controls within and surrounding the firm and its ability to convey the appropriate information to the appropriate parties in a timely manner.

A simplified overview of the information flows within the risk management function is that the staff preparing information report into the CRO, who reports into the Board Risk Committee, and the Chairperson of the Board Risk Committee draws conclusions based on that information, thus providing a degree of assurance to both the full Board and the regulators. According to the interviewees, the regulators are placing growing reliance on this corporate governance mechanism, and require boards to answer directly to them from time to time, as a part of the 'close and continuous' supervision that was discussed earlier.

A distinction between information producers/suppliers and information users/receivers is needed for clarity purposes: I classify NEDs are information users, while CROs are both information users and information producers, depending on which part of their role one looks at, and the people below them, for the purposes of

[25] MI = Management Information: a frequently used abbreviation to describe papers and packs of data that are used by the management and the board.

this research, are seen here as largely information producers. This classification is a result of analysis of practice observations and reviews of literature.

According to the interviewees, NED Risk Committee members attempt to use information from various external sources (e.g. conferences, regulators, consultancy and audit reports), but their primary information providers are within the firm: CROs have a direct reporting line into Board Risk Committees and supply Boards with information packs.

The two categories that were made apparent during the interviews were related to how different NEDs ensure they receive enough information to successfully perform their role: whilst several of the interviewees said they attend conferences, read financial press, use their economies of scope from memberships on other boards and have many informal chats with the CRO as well as with their direct reports, others were more inward-oriented and focused on their own experience and expertise as a source of knowledge, e.g. as an example of the former:

> "I spend a lot of time going round to any sessions that all kinds of other people are running […] because I want to make sure that I'm sufficiently up-to-date that I can ask the right questions" (Interviewee_08, 2014).

In addition to the sources both from within and outside of the business, the importance of face-to-face interaction was acknowledged by the following interviewee, who also listed a number of sources he relies on to get a broader understanding:

> "You can't do it by emails and quantitative data, you actually have to be out in the business, you have to learn what's going on and you have to build a broad perspective from many different sources, be they regulators, be they investment analysts, be they academics and what is happening in the economy and where the emerging risks are" (Interviewee_06, 2014).

While others, when answering the same question, put more emphasis on the value of their intrinsic knowledge when evaluating the various complexities of the business:

> "Essentially it's a role where you use your instincts and emotional intelligence probably more than you use sort of rational IQ. Because you have less than perfect information, you're always less well-informed than the management" (Interviewee_06, 2014).

NEDs demonstrated the understanding of basic agency theory in acknowledging that managers are inevitably better informed about their own business than are NEDs, but combined it with a somewhat less scientific emphasis on instincts and emotional intelligence. Regardless of how NEDs achieve a belief that they are sufficiently informed, information received by the Board in formal instalments prior to their meetings is typically included in so-called "management information packs" which usually contain both qualitative and quantitative data about an organisation. I have participated in the creation of these packs in both organisations I have observed, and they involve a lot of input from various parts of organisation. Therefore, unsurprisingly, there is some heterogeneity across firms in regard to where the information comes from and how it gets processed, although some core information, on accounting profits for example, is fairly standardised across the industry.

> "One of the most conspicuous outcomes of post–financial crisis reflection has been the regulatory imperative that boards need to do a much better job of defining and enforcing their risk appetite" (Power, 2012).

Risk appetite in theory was discussed in Chapter 4, as an object that regulators use as a part of the responsibilisation process. The following section discusses risk appetite as a *process*, rather than a fact, and looks into what goes into its creation and into the measurement of performance against it.

Defining risk appetite is one of the first necessary steps (COSO, 2012b) in the risk management process, which follows risk identification and assessment. After these steps are completed, it is risk management's job to make sure that risks are under control. However, "Boards are expected to provide an oversight role of the risk management systems and processes as well as continuously reviewing both the planning and outcomes of such processes" (Caldwell, 2012). In July 2013, the Financial Stability Board issued a document entitled "Principles for An Effective Risk Appetite Framework" where it outlines the key elements of the risk appetite framework and reporting, as well as defining the roles and responsibilities of those involved in the risk appetite setting and monitoring process. The relevant actors they list are: the board of directors, CEO, CFO, CRO, business-line and entity level management, and internal audit. These actors are in line with the three lines of defence model explained below. Regarding the board's involvement, FSB says that the board members need to: "include an assessment of risk appetite in their strategic discussions […] and ensure adequate resources and expertise are dedicated to risk management as well as internal audit in order to provide independent assurances to the board and senior management." (FSB, 2013a) This signals a strong required involvement in overseeing the processes that surround the risk appetite frameworks.

Without information from within the firm, NEDs would be 'flying blind'; yet securing its accuracy and relevance is problematic. Apart from the complexities of identifying, collecting, analysing and transmitting "appropriate" information, there is an inherent weakness in the process because most of the information NEDs receive comes from sources within the firm, including from the management running the business, whose decisions NEDs are supposed to oversee. Therefore, information could be seen as 'constructing' the NED role. And the providers of information outside line management, despite having significant power and influence in the NED decision-making process, may themselves be influenced by risk takers in the firm and by the profit motive. Even though steps have been taken to divorce the remuneration of risk managers from the profitability of individual business units, CROs are typically rewarded with shares or options, whose value

will be affected by the rate of business expansion, as was discussed in more depth from the observation of remuneration in the previous Chapter.

To allow an examination of the information flow and risk appetite mechanisms, and the links between them, this chapter is structured the following way: after a brief discussion of information intermediaries, information flows are considered within the context of the TLD corporate governance model, and the role of information intermediaries within this process is examined. Then, the role of risk appetite in business strategy as well as the iterative process involved in setting it is explained based on the interview findings and participant observations. The chapter concludes by discussing the challenges that information providers and receivers have to face, which are made more critical by the new weight regulators are placing on these processes.

7.2. INFORMATION INTERMEDIARIES

Information Intermediaries have been spoken about by economists as a part of discussion of market structures. Dzielinski uses information intermediaries as analogous to news agencies within the corporate disclosure regime: their purpose, he says "is providing an objective account of events, especially nowadays when the physical aspect of news dissemination is much less of an issue" (Dzielinski, 2013). A similar use of the term, where information intermediaries are seen as brokers who help reduce the agency problem, has been also applied outside financial markets, where "buyers and sellers don't act independently, but rather exchange information through an intermediary such as a real estate broker or employment agency" (Sass, 1984). Healy and Palepu also discuss information intermediaries which are part of the corporate disclosure infrastructure and are external to the firm – "The credibility of management disclosures is enhanced by regulators, standard setters, auditors and other capital market intermediaries" (Healy & Palepu, 2001). Information intermediaries "such as financial analysts and rating agencies, who engage in private information production to uncover managers' superior information" (Healy

& Palepu, 2001), in their definition, are needed to solve the 'lemons' [26] information asymmetry problem.

This chapter extends the current understanding of information intermediaries as market agents into the space within organisations. It is important to note here that the analytical term 'information intermediaries' is a theoretic construct derived from the academic analysis of observations, not a concept borrowed from practice itself: it is thus a result of focus on the practical information dimension of oversight rather than a presumption.

I use the term information intermediaries to refer to people who are present within firms in order to transmit and transform information and thus enable agency relationships. The core of the problem is the familiar issue of information asymmetry, which is one of the main characteristics of agency theory. But in studies of the principal/agent problem, information flows are often treated as a black box. Hence, this thesis opens that box with the aid of a view from practitioners on both sides of the divide.

> "The Reporting Team [has] a whole bunch of Excel templates […] And output the contents of that spreadsheet in a nice format to *whatever the audience* is that they want to see it. Without the Reporting Team the risk managers, senior risk managers and senior management would not be able to understand and view what their exposures were" (Bank_6, 2012).

Transformation of data into usable information involves more than merely combining information into one report, and in the end has the purpose of directing attention of decision-makers:

---

[26] The 'Lemons Problem' was made popular by the economist George Akerlof who investigated the market for used cars and found that due to quality uncertainty, people with good cars will not place their cars to be sold on the used car market, which results in a decreased quality of the remaining cars, causing a downward spiral. Reliable independent sources of quality re-assurance are needed.

> "The information that we provide is *not just data dump*, it is information that can be viewed and understood: it's about providing that information in a way which […] allows people to understand where their attention should be drawn to. And this is why it's not just a case of setting up the reports and letting them run day in day out, it's a case of constantly evolving to whatever the business needs are" (Bank_6, 2012).

Information intermediaries are the people who create information flows within the oversight structures. They are at the centre of the agency and information asymmetry problem: they simultaneously act to eliminate the problem by providing managers and board members with relevant information, while at the same time also amplifying the problem as they filter, abridge, and edit the information they transmit to higher levels, thus inherently limiting what the overseers see and potentially skewing its meaning.

From the structural perspective, information intermediaries can be understood as the links in the risk oversight process where the information asymmetry problem gets played out. This characteristic became apparent during the participant observations: in an investment bank during the participant observation, there was a newly created position of Chief Operating Officer (COO) to the CRO, whose responsibilities involved overseeing the operations of the risk division, as well as an Enterprise Risk Management division (called "portfolio analysis") that was created in order to gather all the risk management information and make it more suitable for board decision-making. Within the insurance firm, the COO to the CRO was called "head of risk", and the ERM function created the board level papers. They take information from Risk Silo Management (see e.g. Mikes, 2005) and make the information these divisions produce meaningful and usable beyond the excel sheets.

This "filtering" or "editing" process involves deciding what is significant: this passage point between information in organisation and oversight structures is key because it is a standardised process of how information reduction happens. All the information has to be funnelled in some way to get to the board in a useful format. This function is the one in control of the tap that decides how much of it gets to drip to the board. Upward flow is very problematic, because decisions have to be made

about what is material for the oversight function. The people who decide are the critical carriers of the oversight function.

I observed an important variation across firms in this process: during my participant observation in the portfolio analysis group of the major investment bank, I was working for the "oversight" function that decided which information was passed on to management above. I observed that it actually didn't involve much thinking at the analyst level – it was a standardised execution of a pre-determined process of reducing information and passing it up. Which information gets to go up was determined on top, and execution was done in the lower levels.

I found this process to be much more consultative in an insurance firm where I conducted a participant observation in 2013. The ERM group there consisted of 5 people all of whom, regardless of the level of seniority, participated in the discussion and selection of potential risks to be escalated –the suggestions from this list were brought up to the head of risk, and then to the CRO, each of who were able to add or delete points, and it later went back down to the ERM function to prepare the MI itself. This was done, according to an interviewee within that insurance firm, in order to mitigate the risk that "The people doing the filtering may not be senior or insightful enough to identify the important stories. A simple materiality measure will be inadequate. The RC has a forward-looking remit and needs to know not just what big or bad things have happened since the previous MI pack was compiled, but what issues, that may be small now, have the potential to blow up" (Insurance_5, 2013).

7.2.1. TLD: ECOLOGY OF INFORMATION FLOWS

As was demonstrated in the previous chapter, oversight needs to be organised, in order to happen, and the way it has been commonly done is through the Three Lines of Defence framework which, as discussed in Chapter 6, is a conceptualisation of one way - now the dominant way - of organising the practice of oversight. NEDs receive information from each of the three lines, specifically CRO reports directly to the Chairman of the Risk Committee and the risk committee oversees the second line risk function. Within the TLD, information flows permeate every level both within each line and across the functions. The focus of this chapter, in line with the objective of this research to understand how risk oversight functions, is more specifically on management information flows as a narrower dimension at the core of oversight. As a senior risk offer in an insurance firm explained:

> "I see governance as making sure that the right information is going to the right decision maker" (Insurance_1, 2013).

Indeed, it is possible to argue that the TLD is only effective if there is a mechanism for identifying and transferring the right Management Information between lines. For internal audit, this might be seen as less of an issue, since their charter is the equivalent of a search warrant on any other part of the business. The Head of Internal Audit has direct access to the Chair of Audit Committee and the Chair of the Board. For risk control and compliance, there does need to be a level of trust and willingness on the part of the first line to provide time and materials to the second line.

According to a senior interviewee within an insurance firm, "The one sure way for TLD to fail will be in an environment in which the first line keeps its files and mouths closed, providing risk with only what it deems suitable" (Insurance_5, 2013). The interviewee further explained the scenarios that, based on his experience within several major financial instructions, were likely to be the barriers to effective communication between the first and second lines: "if the first line

functional head has much more power than the second line equivalent, or if the risk leadership is not attentive enough to recognise that they are seeing only what the first line chooses to show them, and do not demand information in a helpful manner, or where the 1st line does not see the relevance of the requirements and does not have the time or manpower to carry out all the demands of the 2nd line" (Insurance_5, 2013) .

The board members including NEDs are the receivers at the top of the information hierarchy, usually seen as outside and above the TLD framework: during the participant observations it was evident that they receive the most digested and filtered reports yet use that information to make strategic decisions that might later affect the whole organisation.

At the same time, reporting lines define and construct the TLD – these lines are drawn to reinforce the 'independence' of the different lines of defence. The CRO's reporting line to the Risk Committee is meant to demonstrate some level of independence from the CEO (though this can only be partial as they still have to work together on a day to day basis). The infrastructure of the TLD reporting lines is supported by numerous reporting teams, such as ERM, Risk Oversight, Portfolio Analysis, etc. which vary by institution.

When speaking about the role of the Enterprise Risk Management (ERM) function, an insurance risk executive explained that they are "responsible for maintaining and operationalising the risk policies, monitoring adherence to them, making sure that the appropriate management information flow happens. So aiding governance from a risk perspective" (Insurance_1, 2013). Indeed, the Three Lines of Defence system in its entirety can be seen as defending the firm's risk appetite, because people within those structures not only help set it, but also operationalise it through their actions. The following section explains the definitions and process of risk appetite setting, because it is one of the cornerstones of the risk management and risk oversight process. This centrality makes risk appetite a good example to use in explaining the role of information suppliers and NEDs in the risk oversight process.

7.3. STRATEGIC ROLE OF NEDS

According to COSO's "Enterprise Risk Management — Integrated Framework": "Risk appetite is developed by management and reviewed by the board. Oversight should begin with a studied discussion and review of management's articulation of risk appetite relative to the organization's strategies" (COSO, 2012a). The high-level definitions of risk appetite were discussed in Chapter 4. However, articulation of risk appetite relative to the organisation's strategies is a less straightforward task than it might sound, not least due to the ambiguous nature of the concept (Andersen et al., 2014; Power, 2009). The following section explores how risk appetite is set in practice.

Risk appetite could be defined as a set of metrics, quantifying triggers and limits for a range of exposures. Boards are tasked with approving Risk Policies, which according to a senior interviewee within an insurance firm means that the risk committee: "reviews and approves the words that describe what management should consider when faced with certain business risks" (Insurance_5, 2013). An appetite, in its numerical sense, is a way to make a parts of a risk policy operational and measurable, though some components (e.g. risk culture) might remain qualitative.

The interviewees all shared an appreciation of the centrality of the task to operationalise the risk appetite process, as it is mandated in regulated financial firms, and the close link between risk appetite and strategy. According to Andersen et al, "The risk appetite adopted by a firm should be tied to the firm's strategy as a part of good risk governance. However, the linkage mechanisms are still unclear" (Andersen et al., 2014).

Indeed, the interaction between Risk Appetite and strategy is very direct, as explained e.g. by a Chair of the Board Risk Committee in a major insurance firm:

> "Risk appetite is fundamental to a bank because it's the flipside of the coin of strategy […] risk appetite starts with what type of business do you want to be" (Interviewee_06, 2014).

The close link between the strategy and risk appetite is also there according to the PRA description of Board Responsibilities:

> "A key role for any board is to set the firm's strategy, to ensure that the key goals in that strategy are within the agreed risk appetite and to oversee executive implementation of that strategy" (PRA, 2015b).

NEDs also show some belief that the process of setting risk appetite is meaningful, in spite of its well-understood imperfections, and believe that the oversight process carried out in this way does have a measurable impact on the risks the business takes on. They describe the way the process is intended to operate:

> **"**You hope is that there's a kind of **chain of influence** from the risk appetite policy to the risk function, from the senior executives, so that in every big decision that the organisation has to make there is a risk discussion about how that might change our profile or whatever, which is consistent with the risk appetite" (Interviewee_02, 2014).

They add a distinctive role for the Risk Committee, not as a pure 'policeman' but as a key determinant of the balance between profit-seeking behaviour and risk management, demonstrating an implicit belief in the accuracy and relevance of the information they are provided with, and explain that risk appetite needs to be regularly updated.

> "We make adjustments every year to our risk appetite and our main risk categories and decide how much risk we want to take based on the business model" (Interviewee_09, 2014).

Risk Appetite, since it is related to strategy, is not only about restricting behaviour, but also about encouraging appropriate risk-taking: it is not a purely negative process, defining risks which are 'out of appetite'. A well-positioned risk appetite statement will allow the business to take risks where they are adequately remunerated, and are of a scale which does not threaten the stability of the firm.

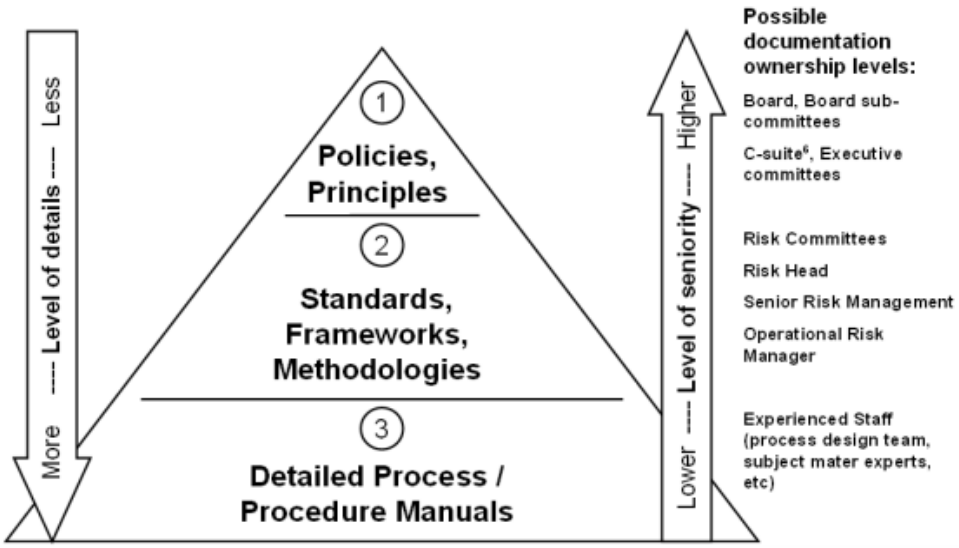
> "You want to see some of your risks in the active zone, otherwise you're not running enough risk in a business based on risk" (Interviewee_09, 2014).

NEDs articulate the dynamic nature of the process, and the need regularly to reassess the relevance of the calibration of the risk appetite in the light of changing business conditions. They also accept that there may be circumstances in which a breach of risk appetite is not necessarily a sign of system failure. A breach may be an indicator of more serious trouble ahead, or may be the trigger for a reassessment of the appropriate degree of risk to be assessed. NEDs explicitly acknowledge that there may be circumstances in which the business moves 'out of appetite':

> "It was completely pointless to have risk appetite levels that you were never in any danger of breaching" (Interviewee_04, 2014).

Therefore NEDs, in theory, get risk data and then add judgements to determine risk appetite. In practice, some interviewees observed the crucial role in this process of managing directors who are closer to business and are thus able to have a stronger influence on the risk appetite setting. "Oversight", by the nature of the term, implies one party looking down at the other, which contains an inherent principal-agent issue because the agent needs to give information to the principal for the principal to be effective. This makes the focus on information flows crucial. "Capacity to assemble information, a key feature of the man-made disasters literature, will be a function of how transaction velocity and complexity create gaps in diagnostic performance measures" (Power, 2007). Exhibit 1 provides an example of the FSA's suggested view on information flows and the level of detail within the various reporting levels of the business.

FIGURE 7.1: FSA'S OPERATIONAL RISK FRAMEWORK



Source: "Enhancing frameworks in the standardized approach to operational risk" (FSA, 2011)

7.3.1. THE INTERACTIVE PROCESS

One of the key purposes of information as discussed here is to facilitate the process of setting and monitoring risk appetite, which is now also officially one of the primary tasks of Boards, though some interviewees mentioned that in reality they do so though the information intermediaries, who thus arguably have significant power in that process. A risk officer in an insurance firm, speaking about the nature of her role, explained: "Our accountabilities increased considerably. Management information is a case in point. In the past we would never be reporting risk matters to the board directly. Now we do it on a monthly basis" (Insurance_6, 2013). Information flows, therefore, can be seen as an indicator of the importance

that is attributed to a certain issue, and risk appetite is now seen as being very important. As one NED put it:

> "[RA is] the model that runs the business and therefore I think no-one will be able to hide behind the idea that risk isn't important. It forces you to put risk right at the top of the agenda" (Interviewee_05, 2014).

After the risk appetite is set, it is then policed by different control mechanisms within the firm.

As discussed in Chapter 5, Board Risk Committees are a more recent formation than Audit Committees, and a Risk Committee does not have as clear a set of routine duties as an Audit Committee has in relation to the financial statements. There is some guidance which gives an indication of the regulators' expectations, but that guidance has itself been evolving rapidly. Therefore, any attempt to describe the process of a risk committee must be accompanied by important caveats. It will inevitably be a snapshot taken at a moment in time, and may not represent practice at all major firms. There are also important differences in process driven by the requirements attached to particular types of regulated firms. For example, bank risk committees have major tasks related to stress tests and capital plans, while insurance companies must produce an ORSA (Own Risk and Solvency Assessment) which is intended to be a kind of 'risk map' for the firm or group as a whole.

There are, nonetheless, some common features of Risk Committee behaviours. The firms I have observed produced schedules of 'top risks' their firm faces, according to a NED who chairs risk committees in two firms. These may be risks self-identified by individual business divisions, or they may originate in the committee itself, or be a mixture of the two. Those top risks, and the steps taken to mitigate them, will be reported to the full Board by the Chair of the Risk Committee. The Risk Committee will also review the risks identified by the regulator, whether they are generalised macroeconomic or market risks embedded in stress tests for banks, or those highlighted in the Bank of England's Financial Stability Review. The Risk Committee will additionally assess the potential impact of regulatory risks, which by definition will not be highlighted by the regulators

themselves. These include the risk that the firm's own controls may be weak, causing it to fail to comply with regulation, and that regulatory actions may raise requirements unexpectedly, or that regulators will retrospectively review past practices against a newer and tougher standard.

All these processes are intended to input to the core function, now mandated and monitored by regulators, of setting a risk appetite for the business as a whole, and also for its component parts/business units. This has arguably now become the most important regular task for the Risk Committee on behalf of the board. There may be ad hoc decisions which have a significant impact on the business – for example putting in place a hedge against potentially damaging unanticipated market moves: e.g. foreign exchange rate protection, or a large equity put, or cases where disagreements between the first and second lines of defence are escalated to board level. Risk appetite can be seen as the gearbox which transmits the Board's view to the individual businesses. Without a clearly defined risk appetite, monitored accurately and as far as possible in real time, a general disposition at the top of the firm that excessive risk taking should be avoided would be no more than an aspiration.

According to one interviewee, overseeing information at the NED level serves a purpose of providing "an assurance that the organisation understands the risks it faces and has a reasonable approach to the mitigation of those. And that you're […] in a no surprises environment" (Interviewee_02, 2014). 'No surprises' means that the risks are within the risk appetite, and risk does not crystallise in unexpected ways.

To illustrate, in a global firm that I have observed, the scale of selling of insurance products with particular characteristics, in this case offering policyholders an equity-linked guarantee, for example, was debated. The hedging of risks was considered, but the committee took the view that hedges rarely offer perfect risk mitigation, unless they are prohibitively expensive. Therefore, the Risk Committee decided in this case to constrain sales growth, even though local business managers, and even their own risk managers, were satisfied with the risk-return trade-off. As a result, the Committee recommended qualified restrictions on sales to the Board, and

after they were approved, those limits were transmitted to local management, who are required to report regularly to the CRO on compliance with them. The CRO will, in turn, report any breaches and exceptions to the Committee, together with a recommendation on the appropriate response. The limits were also notified to regulations, who had expressed concerns about the degree of equity risk being assumed.

This description of the process begs a number of questions: does the information presented to the central risk management function accurately capture the risks of particular exposures or products? Is that information comprehensive? Does it cover all the risks to which business units are exposed? Are the hedging strategies in place, which are intended to reduce the reported risks, robust? In the case of sub-prime mortgage exposures in the years leading to the financial crisis, many banks reported low or non-existent net exposures which were coherent with their stated risk appetite; but the hedges and offsetting short positions they put in place protected them only against modest falls in market prices. The hedging strategies assumed that more significant price falls were out of the question. As a result, the exposures reported up to the Risk Committee (or Audit Committee at that time) were fundamentally misleading and were providing a sense of safety that was misplaced.

That is the background against which the rest of the section examines the in-firm process of information assembly, selection, processing, communicating, and challenging by information intermediaries and the Risk Committee, acting for the Board. The purpose of this section is to emphasise the interactive, iterative, continuous nature of the practice of risk appetite setting. As a Chair of Risk Committee in a FTSE 250 insurance firm explained:

> "Risk appetite statement is a kind of interactive control rather than brittle imperative" (Interviewee_02, 2014).

COSO's thought leadership "Understanding and Communicating Risk Appetite" paper suggests the following simple framework for visualising the continuous and interactive nature of the risk appetite process:

FIGURE 7.2: COSO RISK APPETITE PROCESS

(COSO, 2012a)

The COSO risk appetite process framework in Exhibit 7.1 includes three steps: (1) develop risk appetite, (2) communicate, and (3) monitor. Importantly, that process is shown in a continuous cycle. Both information intermediaries and the board are involved in each of those actions. The rest of this section is structured in accordance with this framework because of its clarity and simplicity, despite the inherent potential over-simplification.

7.3.1.a. Development

NEDs are dependent on the intermediaries in order to obtain the information they need, and indeed one frequently voiced criticism of boards is that most if not

all their information comes from inside the firm. Therefore, even though they bring knowledge and experience, they must rely on internal information only, which has been criticised by the interviewees. On the other hand, information intermediaries within the organisation require NEDs to tell them what they need in order to be able to remain relevant. As another interviewee put it after being asked whether the information he receives is sufficient:

> "There's no one-word answer to that but we keep on trying". (Interviewee_12, 2014)

Although information on business and financial performance originates in the business units and the finance function, from the perspective of risk oversight the risk management function performs the essential role of synthesis and selection. As one interviewee put it:

> "The role of the risk function is to aggregate all that stuff and to help the board in the end decide on the risk appetite, decide on the risk policies and then provide them with one level of assurance that those things are being met" (Interviewee_08, 2014).

A head of the ERM function at the top level of major insurance firm explained that the role of his group in relation to the board risk committee is the following:

> "We would put forward a recommendation for them. So we would say on the basis of a number of considerations, output from the internal model, discussions with senior management, the business unit level top risks. Then the [board] would discuss those and add or delete as appropriate" (Insurance_6, 2013).

This interviewee explained the key role of information intermediaries, as people who consolidate information from various sources within the firm, and then process it into recommendations that help the board decide on the appropriate statements.

The vice-CRO of the same firm, however, saw the ERM role differently and gave it less significance:

> "The people who decide what gets passed on are [CRO and the director level]. Yeah, [ERM group] produced a pack, they drafted it, but actually it goes

through a massive amount of governance. Weeks of governance really before it actually gets finally released" (Insurance_13, 2013).

The fact that even within the same organisation people in neighbouring offices have such different conceptions about the roles within management information production is demonstrative of a fundamental difficulty of studying information intermediaries, since their roles are so open to different interpretations.

When a mid-management level employee within the ERM group spoke about how the priorities about what is communicated to the board are selected, he explained:

> "We give our recommendations of what out of the whole spectrum of information available is most appropriate for them. […] It's quite a subjective view as to what they should be seeing and what not" (Insurance_4, 2013).

When asked about the same issues, a senior internal auditor within the same firm focused on the procedural side of information flows, which involved a lot of collegiate decision making across the departments:

> "There's various structures you have in place to filter information but it is very collegiate. We have a leadership team, a strategy team and all the Executive Directors from all of our regions […] we're not all coming into a room trying to bash out in a day, so there is a lot of work goes on before we get to that stage" (Insurance_2, 2013).

Building up on the explanation of the process of how the ERM group comes up with risk recommendations for the board risk committee to focus on, an interviewee observed:

> "There is a very detailed set of standards that have to be followed […] Typically, we would use the list from the previous year […] then of course the conversations with senior management and the list of BU top risks as well" (Insurance_6, 2013).

While one employee saw some subjectivity in the process, the formation of recommendations is also heavily process-driven according to another. The balance between those two elements, individual decisions and institutional rigour, is something that both information intermediaries and receivers need to manage.

According to a head of insurance risk within a major insurance firm, management information process "is built upon a framework underpinned by the risk appetite - This typically comprises a series of fairly distinct statements, some of which will be both quantitative and instantly calculable" (Insurance_5, 2013).

Based on my observations while producing these statements, these may be portrayed using the Red-Amber-Green status update tables and charts, with red being a breach of risk appetite and amber a warning that some lower threshold has been exceeded and that action may be needed to prevent a future breach. One Chair of risk committee in a FTSE250 firm mentioned that his firm also included blue sections:

> "If the box is blue, we're well within risk appetite. If the box is green, we're within risk appetite. If the box is yellow we're outside of risk appetite but believe we could get back in within a reasonable timeframe" (Interviewee_05, 2014).

In both firms I have been immersed in, the suite of metrics that underpin the risk appetite were referred to as Key Risk Indicators (KRI), and their outputs as levels of risk utilisation: KRIs provided a structured and repeatable basis for risk Management Information. Indeed, a big part of the role was updating the numbers from previous periods based on new data and new calculations, to confirm they remained in accordance with the existing risk appetite.

When it came to the role and production of KRIs, the head of insurance explained: "Given their pivotal role in informing the Risk Committee whether the business has stayed within appetite, their production would typically be subject to more rigorous scrutiny than other MI" (Insurance_5, 2013). The scrutiny is also rigorous due to the fact that NEDs often mentioned that KRIs would be the part of their information packs they prioritised. According to a chairman of one of the largest insurance firms when speaking about key risk indicators:

> "Red, amber and green […] a classic risk committee agenda starts with those slides. So on the aggregate risk profile the conversation is about do we believe

that the outlook in the next 12 months is green? And you can have all the data in the world but do we believe it?" (Interviewee_06, 2014).

This quote demonstrates also the risk committee's need to rely heavily on the Risk Function to ensure that the KRIs are telling the right story and are produced reliably. Based on the conversations with the colleagues at the firms I observed, firms find it easier to demonstrate that they have appropriate processes for data verification and checking than to prove that they are presenting information which accurately captures the firm's risks and allows NEDs to monitor them effectively.

7.3.1.b. Communication

Information flows are needed in order to facilitate the necessary communication upwards between the businesses and the board, as well as across the three lines of defence. As the COO of a risk function in a major investment bank explained, the risk managers' role is not just about understanding and managing, but also importantly about communicating risk to the board:

> "The previous CRO understood the risk exceptionally well – probably better than most people, but wasn't so good at communicating that detail to the senior management and the board. This communicating is important because ultimately the senior management and the board have to understand what our quite complex message is and where it takes the share price" (Bank_17, 2012).

According to Andersen et al., "effective strategic risk management depends on on-going interactions between the strategic planning, risk management, and management control processes where the executives actively communicate with operational managers" (Andersen et al., 2014). Communication is not just a transfer of abridged information, but also involves a level of understanding and prioritisation in order to be able to make the message meaningful:

> "[Producing Risk Oversight reports] in order to get there you can't just copy and paste […] you're relying on that team having knowledge of the other areas. […] You need to change it into what's important and how you put it together in a meaningful message" (Insurance_9, 2013).

Information intermediaries themselves are aware of the fact that NEDs depend on them and of their role within the risk appetite setting process. In particular, it is the key task of the senior risk management team to provide information which allows the Board to set and monitor the firm's risk appetite. Once the information intermediaries digest the issues and communicate their proposals to the board, the board risk committee has to approve and modify the list of top risks, which in turn leads to a transition of ownership from the information intermediaries to the board.

> **"**The role of the group risk department to understand the issues, propose something that is sensible and get the Board's buy in and once the Board has bought in to our proposal, they become the owners. They are ultimately responsible for it and the Board does it via the [Risk Committee] who is part of the Board which is more clued in to the risk issues" (Insurance_1, 2013).

This transformation of ownership that one interviewee described brings the reinforcement and monitoring back to information intermediaries who now have to monitor the progress against this appetite.

Arguably, creating executive summaries is less value adding than spotting oddities in the data. Based on my observations in both firms, over a half of Management Information that goes to the Risk Committee was a filtered version of Management Information that has appeared in packs going to lower level committees in the risk oversight hierarchy within the firm organisation. This observation of course is inherently conditional on the firms being large enough. For example, I received a detailed report on Operational Risk incidents that originally went to a Group Operational Risk committee; and was a part of a group that was asked to make a summary of the more material incidents which then went to a Management or Executive Committee. At the end of this process, Risk Committee got a confirmation that nothing out of appetite has occurred and received a numerical breakdown of the types of incidents over the extended period. This process involves a caveat that before reaching the Risk Committee, it goes through several levels of governance, and therefore introduces material time lags.

7.3.1.c. Monitoring

After the board approves risk appetite, information intermediaries are left in charge of monitoring performance against it, and potentially also overseeing its implementation by line management on behalf of the board. In order to do so, more work is needed at the lower levels to translate it into implementable policies that they can then help the board monitor: quantified limits need to be put in place, and data needed for monitoring has to be collected and analysed against the limits. If a limit is in danger of being breached or has actually been breached, actions need to be taken as well as communicated to the board, which then helps modify future risk appetite limits.

> "The Board will set something which is a bit more high level [...] Then we will try and come up with something quantitative which fits that, then send it back to them and they'll look over it" (Insurance_4, 2013).

This quote shows one of the iterative aspects of the risk appetite process, where translating higher-level suggestions into usable limits is a task of the information intermediaries. Information intermediaries also collect the data required to monitor performance against it, and escalate it to the CRO or the board if necessary:

> "The ERM function ensures that the information is collected from around the business in order to be in a position to know whether we remain within our risk appetite, and also the information is collected in a timely enough way so that the escalation procedures be implemented should you find that you're not within appetite" (Insurance_5, 2013).

The process of preparing, transmitting, and receiving information is continuous and iterative: NEDs react to the information they receive, and request more (or less) information from time to time in a regular dialogue with management. However management, in turn, suggest what data could be focused on. Once the board risk committee approves risk appetite they become its owners, and information intermediaries are in charge of monitoring it and updating their

suggestions for the following period. A caveat here is that "ownership" itself is an unclear concept that is frequently used by practitioners as if it is a fact but the actual meaning is open to interpretation. Throughout the risk appetite process, "ownership" moves iteratively between the board and the intermediaries as discussed above. This process presents a number of challenges that are discussed in the following section.

7.4. PRACTICE CHALLENGES

Although the practitioners interviewed were inclined to interpret their role in a positive light, they accepted the limitations of the process, and mentioned its reliance on good information. The Three Lines of Defence governance structure with the Board Risk Committee overseeing the second line of defence can only make sense if the information presented to the overseers is accurate, sufficient, reliable, and understandable, based on the practitioner understandings: e.g. "Risk management is about the right people taking decisions armed with the right information, timely, relevant, complete, all those kind of things, at the right time, and hopefully that means they'll take the right decisions" (Insurance_15, 2013)". Does it provide a sound basis on which to measure those risks, which are potentially threatening to the firm? There are clear tensions within firms surrounding these problems.

In an attempt to frame these questions, taxonomy below provides a summary of some of the core challenges that were noted by the interviewees:

- Accuracy: are the numbers correct?
- Relevance: do they capture the main big risks which the firm faces?
- Understandability and granularity: are they presented in a way that NEDs can be expected to understand them?
- Sufficiency: is it enough to draw appropriate conclusions?
- Timeliness: how fast are the information flows?

Integrating understanding with literature, information flows are significant in all the three theories that were discussed earlier: agency, management control, and regulation literatures. Relating to the agency theory, directors have an inherent information disadvantage: it is conventional to blame board failures on the information asymmetry, but "board dysfunction can be the result of having either too little or too much information" (Bainbridge & Henderson, 2014). On some boards, "directors are either deprived of information […or] an "indigestible overload of information" is dumped" on them (Ward, 2003). There is an inherent agency problem here that cannot be resolved because both too much and too little information is problematic in its own way.

The accuracy problem might be expected to be unlikely, given the technically advanced data systems and the process of review and analysis involved as the information flows upwards, but there are recent cases where data presented to the Board was wrong: e.g. the RBS capital ratio mistake in October 2014, whereby during the calculation of the Tier 1 ratio for the 2014 European Banking Authority stress test results, "RBS's modelled capital deduction for its Deferred Tax Asset ("DTA") did not adequately reflect these cumulative tax credits within the published Capital Template" (WSJ, 2014). The chairman of the bank was forced to apologise in public for that mistake.

The relevance problem is more serious and was more commonly mentioned by the interviewees who were aware of the agency problem. Information is not neutral and purely objective, but information controllers are crucial and exert major influence. For example, a risk manager within the insurance firm explained that when it comes to supplying information to the board: "We cannot overwhelm them with information. We have to be very selective in what goes to the board. Not selective in the sense of not putting everything […] you can't put everything, you have to put the things that matter, things that have a sense of urgency, and they direct the business" (Insurance_11, 2013).

NEDs themselves are conscious of the problems of relevance and overload, in particular. Most interviewees saw the latter problem as being more difficult than the former. They are concerned that if data are presented to them, they will be assumed to have read them, and future regulatory or legal action will proceed on that basis. So for NEDs information overload is potentially hazardous, as well as time-consuming.

> "We used to get a very, very detailed pack [...] and part of me used to think - oh God, why are we getting all of this stuff?" (Interviewee_04, 2014).

None mentioned that they had been denied information, or had relevant data concealed from them (though logically they may not have been aware of such omission). Since the global financial crisis, management in financial firms have been acutely aware of the personal risks they would run if they were found to have concealed information from the Board, or indeed from regulators (who now have access to board papers if they wish):

> "Information isn't always what you need, because you can […] be deluged with information, thousands and thousands of pages of information. What you need is to make sure that you've identified the key risks that are important to the organisation and that you're being informed of developments around those areas of risk" (Interviewee_09, 2014).

NEDs were mindful about their strategic role in identifying the key risks and accepted that sometimes they themselves insist on a high volume of data, to guard against potential criticism from regulators that they were neglecting to address the necessary level of detail. The suggested solution was to combine breadth and depth by administering so-called "deep-dives", which are particularly detailed reports into certain topics.

> "If you get too much detail […] you cannot see the wood for the trees. One way of dealing with it is to get reasonably high-level data quite often and then have deep-dives. And that's the way it gets dealt with certainly on bigger and more complex organisations" (Interviewee_08, 2014).

Interviewees recognised that it is a part of the responsibility of the risk committee itself to design the information packs so that the information is relevant to their concerns, while not impinging on the managerial space, which is a danger once the reports become too detailed.

> "The issue is to ensure that you don't get sucked into too granular a level because you have to keep the boundary between executive and non-executive. The management run the business, they are responsible for running the business and we hold them to account for running the business" (Interviewee_10, 2014).

However, the exact amount of information required is difficult to determine, and as one interviewee has put it:

> "Everyone always says: I don't want too much detail, but when they don't get detail, they always ask for more details" (Interviewee_02, 2014).

This observation summarises a process that results in a continuous iterative interaction between the management information providers from within the firm and the NEDs.

> "I think that papers that go to a board in most instances should be prepared for the board and not management papers that have just been stuck into a board pack" (Interviewee_09, 2014).

While NEDs were conscious of being careful to not ask for information that does not already exist as it might result in a lot of work at lower levels, at the same time it was also acknowledged that information required for making managerial decisions is different from that needed for the oversight decisions and should be separated. There is also a temptation to provide for NEDs the data which goes to management, even if that is not necessarily relevant to the NEDs particular tasks, and may indeed be too detailed for them readily to digest. Also, it is possible that the information the firm prepares is conditioned by its own perception of the risks it faces, while NEDs may, with their broader experience, see different threats which require different analyses to be prepared.

One practice I observed during my participant observation which can help NEDs is the conduct of post-event reviews. The Board of an investment bank which incurred very large losses on the US sub-prime mortgage securities carried out a review, using an external law firm reporting to the audit committee of Board, to understand how and why the losses had been incurred. One element of the assessment was that the Board (and top management) had not seen data which properly captured the scale of the potential losses. Data on exposures net of hedges had been presented, but those hedges only protected the bank against modest falls in the prices of the securitisations. So the gross exposures, which were not separated or controlled, proved more relevant. That review led to many changes in the way information was collected and presented to the Board.

As is evidenced from the interviews, NEDs show that they see information flows as being a crucial part of risk oversight and are well aware of the problems they have to face, and adopt a variety of strategies to try to overcome them. But in spite of all these strategies there are structural issues, e.g. there is no equivalent in the Risk Committee world of the external audit function, which can provide some independent verification of data. There is also a shortage of meaningful comparative information, which would illuminate the internally produced data, and provide early warnings of trouble ahead: e.g. if a bank's loan losses, or non-performing loans, are escalating more rapidly than that of its principal competitors, that can be an indication that the bank has been lending aggressively or imprudently.

To demonstrate, when discussing the issue of being informed and triangulating data, one interviewee explained:

> "You have to build a multifaceted set of relationships. I would talk the auditors, both external and internal. I would talk to the regulators; they're a great source of information. Fundamentally, you are on the same side as the regulator […] and benchmarking can be a useful input. I'd talk to the consultancies. […] The data that you get presented is one input" (Interviewee_06, 2014).

Relationship-building as an important part of information flows has been emphasised by many interviewees: both in terms of building trust and with

management below them, and external relationships such as regulators, auditors, and consultants. Another positive factor which helps NEDs to be well informed is that UK boards have both executive and non-executive directors which gives "the non-executives greater exposure to the executives and the business strategy, and makes it less possible for executives to hide or withhold information from the board" (Roberts et al., 2005). An important part of being properly informed for directors can still mean reaching outside the organisation for comparative data, as was indicated by several interviewees, but there is a marked contrast between this emerging requirement and the reality of what the interviewees are saying.

7.5. CONCLUSION

Interviewees and consultancy reports regarding their roles show that what risk committees can (and potentially should) do within their responsibilities is the following:

- Ensure that crystallised risks are reported and lessons learned, both for information provision and the definition of risk appetite
- Require management systems to be introduced and assessed independently
- Require that all relevant measurements they consider relevant are used and reported to the Board
- Set a 'risk appetite' in each area and monitor performance against it

But the ability of NEDs to perform their oversight role could be seen as depending crucially on the quality and accuracy of the information they receive. In particular, without information which is relevant, the setting of the firm's risk appetite, and monitoring performance against it, is likely to be difficult if not impossible.

However, despite being such an important part of the corporate governance discussion, most of the information NEDs receive comes from within the firm and

is prepared by 'information intermediaries' who have not been given enough academic attention prior to this chapter. They face tensions in performing their role: they are part of the management of the firm, and informed by its culture and values: they may thus find it problematic to provide information which conflicts with the firm's declared strategy. Perhaps unconsciously, they are influenced by the narrative of strategy and performance articulated by senior management. Also, they often lack the ability to benchmark performance data against competitors and have little incentive to do so.

> "I don't think that basic information flows are difficult, the question is can you get comparative information?" (Interviewee_12, 2014)

It is also useful to note here that if the information is simply wrong it is very difficult for a board to know it is wrong and challenge it. A board can challenge the interpretation that management provides, it can dispute its relevance and complain about timeliness, it can become concerned about not knowing enough to make a clear decision, but unless the board has alternative sources of information or is able to make its own comparisons against expectations, it cannot know that the information is simply wrong, which is why triangulation of information with external sources has been emphasised a number of times. But while NEDs themselves see the need for external sources of information, there is little consistency in their approach to finding it, and ad hoc strategies seem currently to be the favoured option.

Both NEDs and information intermediaries, as well as consultants who support them, show awareness of challenges related to information flows, but have not so far developed strategies to overcome them. The problem is particularly acute in relation to setting and monitoring Risk Appetite. Few NEDs are confident that they have the information which would allow them effectively to perform that function. There is therefore a risk that the Risk Appetite process, seen as crucial by regulators, and accepted as a core demand in the NED role, is not as effective as it should be. Regulators are increasingly challenging firms to prove that the Risk Appetite process is effective and produces practical actions.

This Chapter began by describing the tension between the theory (as it is embodied in the policy statements) and the lived reality of the roles of information intermediaries and non-executives. It has sought to extend current understanding of the agency theory black box of information flow processes by introducing information intermediaries who are internal to the firm and are vital in information production, communication, and monitoring and who therefore empower the boards to perform their roles. The Chapter further suggests a rough taxonomy based on the practitioners' perceptions which allows the quality and relevance of information flows to be assessed (accuracy, relevance, etc). It highlights the 'solutions' which NEDs themselves are considering, which include greater use of comparative data and may in future involve external validation. It argues that without some external input the fundamental agency problem will be very difficult to resolve, despite all the involved parties being aware of it.

CHAPTER 8: DISCUSSION

8.1. CONTRIBUTION AND SUMMARY OF FINDINGS

This thesis has covered oversight in considerable depth, and contributes to knowledge in several specific areas. The primary aim of this research was to understand how the concept of risk oversight related to financial institutions is operationalised in practice, through observations and through actors' explanations of their roles.

This thesis analyses the critical themes that underpin the emergence of risk oversight in practice, particularly since the Walker Report in 2009. While examining the history of risk regulation in the UK, I have identified the principal actors directly and indirectly involved in the risk oversight process, such as the regulators, financial firms, consultancies, audit firms and professional bodies. I have also discussed their interactions with other actors: risk managers, firm management, board members, etc., and the way these interactions have resulted in the creation of risk oversight and three lines of defence as we understand them now.

Through the field immersions, this research identified "risk oversight" as a new area for explicit attention within financial institutions which is distinct from risk management. It presented an overview of how financial firms and their regulators currently conceive the practice of risk oversight at different levels, with a specific emphasis on the risk oversight role of the board of directors.

This thesis has examined the concept of risk oversight in two ways: 1) by reviewing the regulatory and consultancy field discourses and 2) by describing the structures and actions implemented as a response to the above by actors that lead to changes in the practice of risk management and the running of financial institutions.

In the Literature chapter, three distinct intellectual reference points for thinking about risk oversight were explored. These included agency theory as the underlying perspective, regulation theories, and literature on corporate governance and audit committees. The following chapters on Regulators' responsibilisation practices, Board Risk Committees, Three Lines of Defence, and Information Intermediaries, highlighted the practical life of risk oversight.

Chapter 4 on Regulatory perspectives on oversight traced the development of regulatory attitudes to risk oversight and identified the emerging convergence of corporate governance standards and the approaches taken by the financial regulators. While the two strands of regulation begin from different starting points, and have very different scope and legal backing, they now complement each other in the case of regulated financial firms, as both emphasise the key responsibility of boards. Secondly, the chapter showed the process of responsibilisation of NEDs that is intended to promote boards being more involved. Some of the NEDs who find themselves subject to these new definitions of their role and responsibilities are nervous about the consequences. They argue that the restrictions and expectations imposed on them are now so onerous that the willingness of appropriately qualified people to serve on boards may be compromised. The regulatory ideal of NED independence could be seen as posing a tradeoff with competence, because arguably it takes time to become more aware of the firm, but agency theory does not take that tradeoff into consideration.

The so-called 'reversal of the burden of proof' in the new senior management regime applied to banks is seen as a particularly worrying development by NEDs [27]. If well qualified individuals are dissuaded from joining boards – as some argue is already the case – then the paradoxical result may be to diminish the effectiveness of board oversight, which might in turn lead to more intrusive regulation, which would result in a process of de-responsibilisation of NEDs. An overly onerous regime might also lead to overconfidence, with a misplaced belief that the prospect of material failures in oversight can be 'regulated away'. As in any industry, perpetual scrutiny and enhancements of safeguards is required; not a belief that a given process will always militate against the effects of human error. Finally, the establishment of quite prescriptive regulations covering capital requirement calculations or corporate compositions can give rise to a systemic risk, whereby a failure or omission in the regulatory framework, exposed by an unforeseen event, may lead to many firms failing at the same time in similar ways.

Chapter 5 discussed the way NEDs operationalise their roles and oversee the three lines of defence from the outside. They therefore act as both principals and agents at the same time. As the earlier chapters showed, by the design of their role, and their (very) part-time involvement, they are unable to interfere directly at lower levels in the organisation, however assiduous they may be. They are therefore

---

[27] Please note that between the submission of this thesis in September 2015 and its publication in 2016, the reversal of the burden of proof regime suggestion has been abolished by HM Treasure in the October 2015 'Senior Managers and Certification Regime' policy paper: "The senior manager is liable if he or she cannot show the regulator that he or she took the steps that it was reasonable for a person in that position to take to prevent the breach occurring or continuing, thus reversing the normal burden of proof. The government will amend the provisions so that the regulators will only be able to take action if they can show that the individual failed to take the steps that it is reasonable for a person in that position to take to prevent a regulatory breach from occurring. *Therefore concerns over the severity of the original proposals and in particular the implications for the willingness of NEDs to assume Risk Committee chairing roles may need to be softened. The new rules take effect in March 2016*". This thesis, therefore, can be looked at as a historic snapshot.

obliged to place reliance on systems and controls put in place to try to ensure that relevant and unbiased information is presented to them.

The quality of information is a big issue in governance, because information flows to boards come upwards from management, and there is a tension between lived realities and theory about how neat this process is. Another theoretical insight here is a description of how agency-like problems get addressed in the field by actors who are trying to overcome the information asymmetries discussed above. The chapter shows the concept of enforced self-regulation operates through the NEDs who have a relationship with regulator. Audit committee literature could also be extended by looking at the parallels with risk committee's notion of success in chapter 5.

Chapter 6 discusses Three Lines of Defence as a tool of operationalisation of risk oversight, and finds that representations vary depending on the institution that produces them: the big 4 audit firms place a larger emphasis on audit's role than do strategy consultants. Iteratively, over time representations affect practice: practice starts to look like representations, thus creating a self-reinforcing loop. Overall, however, oversight became operationalised in practice through the Three Lines of Defence framework, and indeed it is now so engrained that it appears difficult to speak of risk oversight at the level of financial institutions without speaking of TLD. Aspects of TLD existed before the global financial crisis, and its failures were demonstrated during the crisis to an extent that it is possible to argue that it has failed. Future researchers might ask why, if it existed and failed, it became even more institutionalised as a consequence of the crisis.

The thesis has demonstrated the way a regulatory aspiration for improving risk governance manifests itself through focusing on the more visible aspects of risk oversight, namely Three Lines of Defence structures. However, the practice of risk oversight, seen through the perceptions of NEDs, is more complicated and is not necessarily directly aligned with how regulation suggests it might work. That poses the question: What does it mean for oversight to work? One can put structures in place, but ultimately as this thesis demonstrates, agents such as NEDs and the

information intermediaries who serve them, are the ones who make oversight into something real and consequential.

Chapter 7 on information intermediaries examined the setting of a risk appetite by the board of directors as a process, not an outcome, and discussed practical implementations of what it takes for risk appetite to work. Information intermediaries were shown not to be passive, but rather to actively create the possibility of governance, because they actively manage information, and transfer it from managerial data into information for governance and oversight. While the parallel could be drawn with other internal actors, such as for example management accountants, who produce information for decision-making purposes, explicit separation of information intermediaries in the risk process is analytically useful. The key function of Boards is now conceptualised on being to articulate a risk appetite, which will allow the firm to prosper in good times and survive in bad times. That framework is intellectually appealing but will only work well if the information needed to define and monitor the risk appetite is accurate and relevant. The chapter was more speculative than the others, and raised a number of questions for future research.

This thesis contributed to knowledge by tracing the dynamics between the content of normative and regulatory pronouncements and the practices and interpretations that follow, and produced new empirical data on the newly emergent phenomenon of risk oversight. Specific contributions to existing literature are threefold. First, in relation to the *agency literature*, the discussion of NEDs shows how they act as both agents and principals and the tensions and tradeoffs to which this gives rise. Second, in relation to the literature on, *enforced self-regulation,* the thesis demonstrates the convergence of financial regulation and corporate governance on risk oversight and NED responsibilities. Third, in relations to the *audit committee literature* the thesis shows how risk committes are both similar to and different from audit committees.

8.2. PRACTICE IMPLICATIONS, LIMITATIONS, FUTURE RESEARCH

As a regulatory object, risk oversight formed over time, and "exploded" after the financial crisis. This thesis calls for a deeper investigation of causal relationships between the way organisational structures were implemented and the organisational outcomes. Specifically, one could investigate the issues related to the development of ERM over time, and also deepen the understanding of information flows and risk appetite processes that were touched upon in Chapter 7. It would also be fruitful to investigate organisational responses to more narrow issues such as cyber risks or reputational risks.

While the data set was strong and included a number of in-depth interviews, its qualitative nature resulted in the typical limitations: for example, I have not conducted a survey, nor gathered big enough data samples to be able to give wider recommendations about best practice or make a judgement about what does and does not work. Additionally, no cross-country comparisons were given, which could also be a relevant future research area.

The research was not intended to be a longitudinal pre-and post- global financial crisis study, which limits its ability to make extrapolations about change beyond the actors' descriptions of what had changed. Theory of crises could be applied here in order to examine how oversight has developed and whether the trajectory could have been different had there been some different type of global financial crisis. Risk oversight is an interesting area of future research because it has a very high degree of practical relevance, while also being an underexplored area in academic terms.

Other unanswered practice questions include: how can the new oversight regime avoid repeating the mistakes that it is put in place to avoid, and ensure it does not lead to an overly strong sense of security? How can the financial industry,

which relies on taking measured risks, avoid the moral hazard of feeling too safe, assuming the institution cannot fail?

One of the objects of regulatory attention has been restitution plans, informally called 'living wills', whereby firms have to explain their plan for handling orderly default. Examining how living wills affect the practice of financial institutions, especially after one of the banks fails, would be an interesting focus for future research.

One could also examine Basel III and Solvency II in more detail, particularly in terms of their effect on boards of directors, and their oversight role; and be more critical of the fact that risk managers might be becoming data processors due to the amount of time they spent on capital requirements.

Another aspect of regulatory attention has been on stress tests: the Bank of England's latest stress test[28] requirements ask banks to test against a possible dramatic deterioration in global economic conditions and to demonstrate their resilience[29]. While the banks are producing elaborate reports, one question that

---

[28] Source: http://www.bankofengland.co.uk/financialstability/pages/fpc/stresstest.aspx

[29] The test was run for the first time in 2014 and included the eight largest banks and building societies. Six banks and Nationwide building society will be tested this year. Together they account for around 70% of the stock of lending to UK businesses and around 75% of the stock of UK mortgage lending.

The apocalyptic scenario laid out by the Bank includes a combination of the oil price at US$38 per barrel, Chinese residential property prices falling 35% below their level at end-2014, domestic consumption and investment both falling, aggregate euro-area real GDP growth at -2.1%. In Europe, the euro depreciates by 25% against the US dollar, and residential property prices fall by 20%... "It is not a set of events that is expected, or likely, to materialize", the Bank reassuringly emphasises, but "rather, it is a coherent 'tail-risk' scenario that has been designed specifically to assess the resilience of UK banks and building societies to a deterioration in global economic conditions".

arises is: how does that kind of exercise fit into the current approach to risk management and risk oversight?

Having described the apocalyptic scenarios as a part of stress testing, what will banks and their regulators do about it in the future? Simply note that if all these trends occur at once they will be obliged to de-risk their balance sheets further, against a scenario which the Bank itself says it does not expect to see? Or will an understanding of the available managerial courses of action in such scenarios improve board risk oversight? How can the risk committees continue being relevant and useful? Are they indeed relevant and useful?

The variation in the meaning and interpretations of 'risk oversight' was vast, and I did not expect to find a standard application of the term. This thesis has shed light on this concept and discussed how oversight is done in practice through dissecting it at the level of regulators, NEDs, and actors within the firms. As demonstrated above, ambiguity about what constitutes risk oversight is one of the features of the term. This plurality of multi-level accountabilities could be explored in more depth by future researchers.

Layers of complicated information flows present major problems in financial institutions, but so far there is little sign that these problems have been resolved. It is likely that there will need to be new external sources of information if the Risk Oversight function overseen by the Board is to deliver the high expectations placed upon it, and some interviewees have indicated a demand for independent advisory services like external audit.

To answer the question in the title: are the changes in risk oversight within financial regulation really like closing the stable door after the horse has bolted? Some believe that regulators have overreacted. From a laissez-faire pre-crisis regime, they have moved to a highly prescriptive and top-down set of requirements, imposing burdens on boards of directors which sit uneasily with their role as protectors of shareholder interests. The perspective emerging from this research is somewhat different. Regulators have attempted to put in place mechanisms which will better cope with issues that might emerge in the next crisis.

It would be unreasonable to expect the next crisis to be the same as the last one: with identical root causes or the way these causes manifest themselves to result in a crisis. However, the systems in place now are attempting to cover a wider range of scenarios and to handle problems better, not just replaying past events. While risks such as a credit crunch and a lack of market confidence that materialised in the last crisis are still being considered, other major risks yet to emerge, such as cyber risks or insurers' illiquidity are now being captured and better understood.

There is a risk that regulators seek to guard against 'four of the next three crises[30]', or in other words overregulate with negative consequences for risk taking and capital availability. The extensive focus on orderly default demonstrates the regulatory stance that firms must be allowed to fail, but to do so without causing overly strong systemic repercussions. Regulators may therefore see themselves as requiring flood defences to be put in place – generic safety measures that are designed to limit the damage but without assuming the exact source of the problem.

Therefore, flood defence is a better metaphor than 'closing the stable door' to assess the intended consequences of the new system. The new oversight structures have introduced discipline that is intended to protect against a wider range of potential conceivable risks. Only time will tell whether they have succeeded.

---

[30] Jacob A. Frenkel asks: "Should we design a system that is capable of eliminating three out of the next four crises or should we design a system that is designed to eliminate four out of the next three crises? It is not a game of words - there is a big difference. If you eliminate four out of the next three crises you have overintervened, you have prevented free enterprise from operating - you have over-regulated. You will look good because no bank has been closed during your regime. But you have not allowed free enterprise to thrive. If you have eliminated three out of four crises then, yes, life is risky but you should be able to handle it. I think that is a very important issue - what systems we want, and knowing that we will never be able to eliminate all risk" – Distinguished Lectures Series; Warsaw, 25 November 2002 (Frenkel, 2002)

APPENDICES

APPENDIX I: TLD INTERVIEW QUESTIONS

[This firm] describes its Risk Management approach as 3-lines of defence.

- What do you think it means? What do you think about three lines of defence?
- Whom do you report to? Whom is your team/function accountable to?
- Should 2nd line (RM) be doing *management* or *oversight*?

Interaction between lines:

- How clear are the separations?
- How are disagreements between the lines escalated and resolved?
- Do you feel that you are in the position to overrule 1st line? Are reporting lines such that issues are sorted on your level, or is it typically escalated, negotiation is done at the top, and then the decision is brought down again?
- How do you interact with those in the 3rd line?

Information Flows:

- How does the information you produce enable the board to function?
- Do you think you get all the information you need to do your job effectively?
- Is most information you use generated within the business, or are you using external sources?
- How much *control* do you have over what information you get?

APPENDIX II: INTERVIEW QUESTIONS FOR NEDS

ABOUT THE ROLE

- What are the main challenges of being a non-executive director (+ info – how long, what other firms, etc)
- What does it mean to be a successful NED
- To whom are you responsible?
- How do you balance your oversight vs. management roles?
- What can a board risk committee accomplish and for whom?
- When you say you are doing oversight (assurance etc), what is it that you are doing exactly?

RELATIONSHIP WITH THE CRO

- What are the reporting lines and relationships between you and the CRO?
- Do you feel that executive management support you in your non-executive role?
- [Is the CRO on your board?] Do you think CRO should be on the board, and does it make any difference?

QUALITY OF INFORMATION

- What is the goal of information – what do you want to achieve with the information you are getting?
- Some organisations have adapted three lines of defence model of governance. What are your thoughts about it? [What output do you see from the three different lines? What reports are you getting?]
- Do you think the information you get is sufficient to perform your role?
- How do you gain confidence that you are seeing the organisation as it really is?
- What specific information is particularly useful for your job?
- How much influence do you have over the information you get?
- What is the role of risk appetite: does it change decision-making behaviours?

APPENDIX III: LIST OF PUBLICATIONS

- **What the Sony hack can teach risk committees**
  (Financial Times, Dec 31, 2014, co-authored with Howard Davies)

- **The dilemma of defining risk appetite in banking**
  (Financial Times, Sep 9, 2014, co-authored with Howard Davies)

- **Audit is no longer the chore the board dreads most**
  (Financial Times, July 28, 2014, co-authored with Howard Davies)

- Book Review: "**Managing Risk and Opportunity: the Governance of Strategic Risk Taking**" by Torben Andersen, Maxine L. Garvey, Oliviero Roggi
  (LSE Review of Books June 27, 2014)

- Book Review: "**Risk: A Study of its Origins, History and Politics**" by Matthias Beck and Beth Kewell
  (LSE Review of Books March 22, 2014)

- **Risky business set to grow**
  (Financial World, December 2013, co-authored with Howard Davies)

- **Banks need to question their 'three lines of defence'**
  (Financial Times, July 9, 2013, co-authored with Howard Davies)

- **French critics of allowing foreign-language instruction are fighting lost battles**
  (Times Higher Education, June 13, 2013, co-authored with Howard Davies)

- **How to avoid reputational ruin: a guide for banks**
  (Financial Times Oct 3, 2012, co-authored with Howard Davies)

REFERENCES

Abbott, A. (1988). The system of professions. An essay on the division of expert labor. *Chicago: University of Chicago Press, 1*(20), 33-34.

Abbott, L. J., Parker, S., & Peters, G. F. (2010). Serving two masters: The association between audit committee internal audit oversight and internal audit activities. *Accounting Horizons, 24*(1), 1-24.

Acheson, N. (2004). *Two paths, one purpose : voluntary action in Ireland, north and south ; a report to the Royal Irish Academy's Third Sector research programme*. Dublin: IPA ;.

Adams, R., Hermalin, B. E., & Weisbach, M. S. (2008). The role of boards of directors in corporate governance: A conceptual framework and survey: National Bureau of Economic Research.

Ahmad, Z., & Taylor, D. (2009). Commitment to independence by internal auditors: the effects of role ambiguity and role conflict. *Managerial Auditing Journal, 24*(9), 899-925.

Alford, R. (2010). Some help in understanding Britain's banking crisis, 2007-09: Financial Markets Group, LSE.

Alvesson, M. (2003). Methodology for close up studies–struggling with closeness and closure. *Higher education, 46*(2), 167-193.

Andersen, T. J., Garvey, M., & Roggi, O. (2014). *Managing Risk and Opportunity: The Governance of Strategic Risk-taking*: Oxford University Press.

Anderson, S. W., & Widener, S. K. (2006). Doing quantitative field research in management accounting. *Handbooks of Management Accounting Research, 1*, 319-341.

Aram, J. D., & Salipante, P. F. (2003). Bridging scholarship in management: Epistemological reflections. *British Journal of Management, 14*(3), 189-205.

Arcot, S., & Bruno, V. (2006). In letter but not in spirit: an analysis of corporate governance in the UK. *Available at SSRN 819784*.

Ashby, S., Palermo, T., & Power, M. (2012). Risk culture in financial organisations: an interim report. *LSE*.

Attride-Stirling, J. (2001). Thematic networks: an analytic tool for qualitative research. *Qualitative research, 1*(3), 385-405.

Baiman, S. (1990). Agency research in managerial accounting: A second look. *Accounting, Organizations and Society, 15*(4), 341-371.

Bainbridge, S. M., & Henderson, M. T. (2014). Boards-R-Us: Reconceptualizing Corporate Boards. *Stanford Law Review, 66*(5), 1051.

Baldwin, R., & Black, J. (2008). Really responsive regulation. *The Modern Law Review, 71*(1), 59-94.

Baldwin, R., Cave, M., & Lodge, M. (2010). *The Oxford handbook of regulation*: Oxford Handbooks Online.

Baldwin, R., Hood, C., Rothstein, H., Hutter, B. M., & Power, M. (2000). Risk management and business regulation.

Bank for International Settlements. (1999). Enhancing Corporate Governance for Banking Organisations. *September, Basel Committee on Banking Supervision*(http://www.bis.org/publ/bcbs56.pdf).
Bank for International Settlements. (2012). The internal audit function in banks. *June, Basel Committee on Banking Supervision*(http://www.bis.org/publ/bcbs223.pdf).
Bank of England. (2013). News Release 08 July 2013 - PRA and FCA welcome Internal Audit guidance. http://www.bankofengland.co.uk/publications/Pages/news/2013/087.aspx.
Bank of England. (2014). The Financial Policy Committee's review of the leverage ratio. http://www.bankofengland.co.uk/financialstability/Documents/fpc/fs_cp.pdf.
Bank of England. (2015). Fair and Effective Markets Review. http://www.bankofengland.co.uk/markets/Documents/femrjun15.pdf.
Bank of England, FSA, & Treasury, H. (2000). Memorandum of Understanding.
Barker, R., Hendry, J., Roberts, J., & Sanderson, P. (2012). Can company-fund manager meetings convey informational benefits? Exploring the rationalisation of equity investment decision making by UK fund managers. *Accounting, Organizations and Society, 37*(4), 207-222.
Bartunek, J. M., & Louis, M. R. (1996). *Insider/outsider team research*: Sage Thousand Oaks, CA.
Barwell, R. (2013). *Macroprudential Policy: Taming the wild gyrations of credit flows, debt stocks and asset prices*: Palgrave Macmillan.
Bauer, M. W., & Gaskell, G. (2000). *Qualitative researching with text, image and sound: A practical handbook for social research*: Sage.
Baysinger, B., & Hoskisson, R. E. (1990). The composition of boards of directors and strategic control: Effects on corporate strategy. *Academy of Management review, 15*(1), 72-87.
BBC. (2001). New powers for City watchdog. http://news.bbc.co.uk/1/hi/business/1684872.stm.
BBC. (2010). BBC Radio 4 - Analysis - "A price worth paying?" *1 February, Retrieved Nov 1, 2013*.
Beasley, M. S., Carcello, J. V., Hermanson, D. R., & Neal, T. L. (2009). The Audit Committee Oversight Process*. *Contemporary Accounting Research, 26*(1), 65-122.
Beasley, M. S., Frigo, M. L., Fraser, J., & Simkins, B. J. (2010). ERM and its role in strategic planning and strategy execution. *Enterprise Risk Management*, 31-50.
Bédard, J., & Gendron, Y. (2010). Strengthening the financial reporting system: Can audit committees deliver? *International journal of auditing, 14*(2), 174-210.
Bennis, W. G., & O'Toole, J. (2005). How business schools lost their way. *Harvard Business Review, 83*(5), 96-104.
Berelson, B. (1952). Content analysis in communication research.
Bernanke, B. (2008). *Reducing systemic risk.* Paper presented at the Federal Reserve Bank of Kansas City's Annual Economic Symposium, Jackson Hole, Wyoming.
Bernanke, B. (2011). *Implementing a macroprudential approach to supervision and regulation.* Paper presented at the 47th Annual Conference on Bank Structure and Competition, Chicago, Illinois, May.
Bernanke, B. S. (1983). Non-monetary effects of the financial crisis in the propagation of the Great Depression: National Bureau of Economic Research.
Bernard, H. R. (2011). *Research methods in anthropology*: Rowman Altamira.
Bessis, J. (2011). *Risk management in banking*: Wiley. com.
Bhimani, A. (2008). Making corporate governance count: the fusion of ethics and economic rationality. *Journal of Management & Governance, 12*(2), 135-147.

Bhimani, A. (2009). Risk management, corporate governance and management accounting: Emerging interdependencies. *Management Accounting Research, 20*(1), 2-5.
Bhimani, A., & Langfield-Smith, K. (2007). Structure, formality and the importance of financial and non-financial information in strategy development and implementation. *Management Accounting Research, 18*(1), 3-31.
Bhimani, A., Ncube, M., & Sivabalan, P. (2015). Managing risk in mergers and acquisitions activity: beyond 'good'and 'bad'management. *Managerial Auditing Journal, 30*(2), 160-175.
BIS. (2010a). Principles for enhancing corporate governance - Consultative Document *March,* http://www.bis.org/publ/bcbs168.pdf.
BIS. (2010b). Principles for enhancing corporate governance - final document. *October,* http://www.bis.org/publ/bcbs176.pdf.
Black, J. (2001). Decentring regulation: Understanding the role of regulation and self-regulation in a "post-regulatory" world. *Current legal problems, 54*(1), 103-146.
Black, J. (2002). Critical reflections on regulation. *Austl. J. Leg. Phil., 27*, 1.
Black, J. (2004). The Development of Risk Based Regulation in Financial Services: Canada, the UK and Australia. *ESRC Centre for the Analysis of Risk and Regulation Research Report*.
Black, J. (2010). The rise, fall and fate of principles based regulation.
Bloor, M., & Wood, F. (2006). *Keywords in qualitative methods: A vocabulary of research concepts*: Sage.
Bonisch, P. (2013). Excuse me, how many lines of defence? The new financial Maginot lines... *March,* http://paradigmrisk.wordpress.com/2013/03/18/excuse-me-how-many-lines-of-defence-the-new-financial-maginot-lines/.
BRC, & NYSE. (2002). *Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees Report*.
Brodkey, L. (1987). Writing critical ethnographic narratives. *Anthropology & Education Quarterly, 18*(2), 67-76.
Bromwich, M. (2006). Economics in management accounting. *Handbooks of Management Accounting Research, 1*, 137-162.
Burden, P. (2008). Three lines of defence model. *ACCA - Internal Audit Bulletin, February*(http://archive.newsweaver.com/accaiabulletin/newsweaver.co.uk/accaiabulletin/e_article00102615464e4.html).
Cadbury. (1992). *Report of the committee on the financial aspects of corporate governance* (Vol. 1): Gee.
Caldwell, J. (2012). A framework for board oversight of enterprise risk. *The Canadian Institute of Chartered Accountants* (http://www.cica.ca/focus-on-practice-areas/governance-strategy-and-risk/directors-series/director-briefings/item66262.pdf).
Carlile, P. R. (2002). A pragmatic view of knowledge and boundaries: Boundary objects in new product development. *Organization science, 13*(4), 442-455.
Carmassi, J., Gros, D., & Micossi, S. (2009). The Global Financial Crisis: Causes and Cures. *JCMS: Journal of Common Market Studies, 47*(5), 977-996.
Carpenter, J. N. (2000). Does option compensation increase managerial risk appetite? *The journal of finance, 55*(5), 2311-2331.
Carter, C. B., & Lorsch, J. (2013). *Back to the drawing board: Designing corporate boards for a complex world*: Harvard Business Press.
Clarke, D. C. (2007). Three concepts of the independent director. *Del. J. Corp. L., 32*, 73.
Cohen, J. R., & Holder-Webb, L. L. (2006). Rethinking the influence of agency theory in the accounting academy. *Issues in Accounting Education, 21*(1), 17-30.

Commission, E. (2010). Corporate Governance in Financial Institutions: Lessons to be drawn from the current financial crisis, best practices. *June,* http://ec.europa.eu/internal_market/company/docs/modern/sec2010_669_en.pdf.
Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative sociology, 13*(1), 3-21.
COSO. (2010). Board Risk Oversight – a progress report. *December,* http://www.coso.org/documents/Board-Risk-Oversight-Survey-COSO-Protiviti_000.pdf.
COSO. (2012a). Understanding and Communicating Risk Appetite. http://www.coso.org/documents/ERM-Understanding_Communicating Risk Appetite-WEB_FINAL_r9.pdf.
COSO. (2012b). Understanding and Communicating Risk Appetite.
COSO. (2014). COSO: about us. http://www.coso.org/aboutus.htm.
Daily, C. M., Dalton, D. R., & Cannella, A. A. (2003). Corporate governance: decades of dialogue and data. *Academy of management review, 28*(3), 371-382.
Davies, H. (2010). The Financial Crisis: Who is to blame? *Polity Press*.
Davies, H., & Zhivitskaya, M. (2014). The dilemma of defining risk appetite in banking. *FT*(http://www.ft.com/cms/s/0/8363a88c-380c-11e4-a687-00144feabdc0.html - axzz3gGlYXl5A).
Davies, M. (2011). Women on Boards. *https://*http://www.gov.uk/government/uploads/system/uploads/attachment_data/file/31480/11-745-women-on-boards.pdf.
de Larosière, J. (2009). The High-level Group on Financial Supervision in the EU. *February,* http://ec.europa.eu/internal_market/finances/docs/de_larosiere_report_en.pdf.
Delamont, S. (2004). Ethnography and participant observation. *Qualitative research practice*, 217-229.
Deloitte. (2009). Assessing Enterprise Risk Management. *May,* http://www.corpgov.deloitte.com/binary/com.epicentric.contentmanagement.servlet.ContentDeliveryServlet/CanEng/Documents/Risk Oversight/AssessingEnterpriseRiskManagement.pdf.
Deloitte. (2010). The Board and Risk Oversight: Increasing Transparency Through Proxy Disclosure. *NACD Directorship, 36 (5)*.
Deloitte. (2013a). Internal Audit in Financial Services. http://www.deloitte.com/view/en_LU/lu/market-challenges/internal-governance-risk-management/index.htm - .UfGm2T6xBF8.
Deloitte. (2013b). Internal Audit in Insurance breakfast briefing. *September*.
Demb, A., & Neubauer, F. (1992). The corporate board: confronting the paradoxes. *Long range planning, 25*(3), 9-20.
Dent, J. F. (1991). Accounting and organizational cultures: a field study of the emergence of a new organizational reality. *Accounting, Organizations and Society, 16*(8), 705-732.
Dentons. (2012). The Federal Reserve Board's Proposed New Risk Management Requirements for Firms Requiring Enhanced Supervision. http://www.dentons.com/en/insights/alerts/2012/october/22/the-federal-reserve-boards-proposed-new-risk-management-requirements-for-firms-requiring-enhanced-s.
DeWalt, K. M., & DeWalt, B. R. (2010). *Participant observation: A guide for fieldworkers*: Rowman Altamira.

DeZoort, F. T. (1998). An analysis of experience effects on audit committee members' oversight judgments. *Accounting, Organizations and Society, 23*(1), 1-21.
Donaldson, L. (1990). The ethereal hand: Organizational economics and management theory. *Academy of management Review, 15*(3), 369-381.
Donaldson, L., & Davis, J. H. (1991). Stewardship theory or agency theory: CEO governance and shareholder returns. *Australian Journal of management, 16*(1), 49-64.
Douglas, M. (1986). The Social Preconditions of Radical Scepticism in Power, Action and Belief. A New Sociology of Knowledge? *Sociological review*(32), 68-87.
Duffie, D., & Pan, J. (1997). An overview of value at risk. *The Journal of derivatives, 4*(3), 7-49.
Dzielinski, M. (2013). The role of information intermediaries in financial markets. *Swedish House of Finance Research Paper*(13-02).
ECIIA. (2012). Reinforcing audit committee oversight through global assurance. *Corporate Governance Insights, May*.
Economist. (2000). Delayed gratification, http://www.economist.com/node/302494.
Eisenberg, M. A. (1999). Corporate law and social norms. *Columbia Law Review*, 1253-1292.
Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of management review*, 57-74.
Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of management journal, 50*(1), 25-32.
Ellul, A., & Yerramilli, V. (2013). Stronger risk controls, lower risk: Evidence from US bank holding companies. *The Journal of Finance, 68*(5), 1757-1803.
Ernst&Young. (2012). Risk Management for Asset Management. http://www.ey.com/Publication/vwLUAssets/2012_EMEIA_asset_management_risk_survey/$FILE/Risk_Management_for_AM_EY_Survey_2012.pdf.
EY. (2013a). Global Consumer Banking Survey 2012.
EY. (2013b). The Three Lines of Defense in Effective Risk Management and Control.
EY. (2015). A focus on value creation and regulatory oversight: 2015 insurance CRO Survey.
Fama, E. F. (1980). Agency Problems and the Theory of the Firm. *The journal of political economy*, 288-307.
FCA. (2015). Financial Conduct Authority confirms approach to improving responsibility and accountability in the banking sector. http://www.fca.org.uk/news/approach-to-improving-responsibility-and-accountability-in-the-banking-sector, *March*.
FED. (2014). Final Regulation Implementing Dodd-Frank Section 165 Enhanced Prudential Standards for Large US and Non-US Banking Organizations.
Ferreira, L. D., & Merchant, K. A. (1992). Field research in management accounting and control: a review and evaluation. *Accounting, Auditing & Accountability Journal, 5*(4).
Fleischer, V. (2010). Regulatory arbitrage. *Tex. L. Rev., 89*, 227.
Flick, U. (2014). *An introduction to qualitative research*: Sage.
Fligstein, N. (1993). *The transformation of corporate control*: Harvard University Press.
FOO, S. L. (2012). SGX Listing Rule 1207 (1): Challenegs & Opportunities for CAEs.
FRC. (2010a). The UK Approach to Corporate Governance. *October*.
FRC. (2010b). THE UK CORPORATE GOVERNANCE CODE. *June,* http://www.frc.org.uk/Our-Work/Publications/Corporate-Governance/The-UK-Corporate-Governance-Code.aspx.
FRC. (2011a). Boards and risk. *September*.

FRC. (2011b). Developments in Corporate Governance. *December,* http://www.frc.org.uk/Our-Work/Publications/Corporate-Governance/Developments-in-Corporate-Governance-2011-The-impa.aspx.
FRC. (2014a). Guidance on Risk Management, Internal Control and Related Financial and Business Reporting. *UK Corporate Governance Code*.
FRC. (2014b). The UK Corporate Governance Code. *https://*http://www.frc.org.uk/Our-Work/Publications/Corporate-Governance/UK-Corporate-Governance-Code-2014.pdf.
FRC. (2015). Financial Reporting Council: about us. *https://*http://www.frc.org.uk/about.
Frenkel. (2002). *The Global Economy: Strong Fundamentals versus Financial Vulnerabilities*. Paper presented at the Distinguished Lectures Series n. 9, Warsaw.
FSA. (1997a). Financial Services Authority: an outline. *October,* http://www.fsa.gov.uk/pubs/policy/launch.pdf.
FSA. (1997b). FSA: About us. http://www.fsa.gov.uk/about/who/history.
FSA. (1998). Risk based approach to supervision of banks.
FSA. (2003). Building a framework for operational risk management: the FSA's observations. *July,* http://www.fsa.gov.uk/pubs/policy/ps142_2.pdf.
FSA. (2004). Speech by Kari Hale: Challenges to the UK Banking Sector. *November*.
FSA. (2006). The FSA's risk assessment framework. *August,* http://www.rdec.gov.tw/public/Data/851414194871.pdf.
FSA. (2007). Principles Based Regulation: Focusing on the outcomes that matter. http://www.fsa.gov.uk/pubs/other/principles.pdf.
FSA. (2008). Annual Report 2008/09.
FSA. (2009a). Business Plan 2009/10.
FSA. (2009b). "The Turner Review: A regulatory response to the global banking crisis". *March,* http://www.fsa.gov.uk/pubs/other/turner_review.pdf.
FSA. (2010a). Effective corporate governace: Significant influence controlled functions and the Walker Review. *September, Policy Statement*.
FSA. (2010b). Effective corporate governance: Significant influence controlled functions and the Walker review. *January, Consultation Paper*.
FSA. (2011). Enhancing frameworks in the standardised approach to operational risk – Guidance note. *January,* http://www.fsa.gov.uk/pubs/guidance/guidance11.pdf.
FSB. (2013a). Principles for An Effective Risk Appetite Framework. *July,* http://www.financialstabilityboard.org/publications/r_130717.pdf.
FSB. (2013b). Principles for An Effective Risk Appetite Framework. http://www.financialstabilityboard.org/wp-content/uploads/r_131118.pdf.
FSMA. (2000). Financial Services and Markets Act 2000 (FSMA). http://www.legislation.gov.uk/ukpga/2000/8/contents.
GARP. (2015). "GARP by Numbers". *https://*http://www.garp.org/ - !/frm/about.
Gendron, Y. (2009). Discussion of "The Audit Committee Oversight Process": Advocating Openness in Accounting Research. *Contemporary Accounting Research, 26*(1), 123-134.
Gendron, Y. (2014). Working paper: The Construction of Risk Management Credibility within Corporate Boardrooms. *Presented in LSE, Nov*.
Gendron, Y., & Bédard, J. (2006). On the constitution of audit committee effectiveness. *Accounting, Organizations and Society, 31*(3), 211-239.
Gieryn, T. F. (1983). Boundary-work and the demarcation of science from non-science: Strains and interests in professional ideologies of scientists. *American sociological review*, 781-795.

Gillham, B. (2005). *Research Interviewing: The Range Of Techniques: A Practical Guide*: McGraw-Hill International.
Goodhart, C. (2009). Procyclicality and financial regulation. *Estabilidad Financiera, 16*, 9-20.
Gordon, J. N. (2007). The rise of independent directors in the United States, 1950-2005: Of shareholder value and stock market prices. *Stanford Law Review*, 1465-1568.
GrantThornton. (2011). Corporate Governance Review 2011: A changing climate - Fresh challenges ahead. http://www.grant-thornton.co.uk/pdf/corporate_governance.pdf.
Greenbury, R. (1995). Directors' Remuneration: Report of a Study Group. *July, Confederation of British Industry*.
Guadalupe, M., Li, H., & Wulf, J. (2013). Who lives in the C-suite? Organizational structure and the division of labor in top management. *Management Science, 60*(4), 824-844.
Gupta, A. K., & Govindarajan, V. (1991). Knowledge flows and the structure of control within multinational corporations. *Academy of management review, 16*(4), 768-792.
Hall, M. (2010). Accounting information and managerial work. *Accounting, Organizations and Society, 35*(3), 301-315.
Hall, M., Mikes, A., & Millo, Y. (2013). *How do risk managers become influential? A field study in two financial institutions*: Working Paper, Harvard Business School, October 17.
Hall, M., Mikes, A., & Millo, Y. (2015). How do risk managers become influential? A field study of toolmaking in two financial institutions. *Management Accounting Research, 26*, 3-22.
Hampel, R. (1998). Final Report: Committee on Corporate Governance. *January*.
Hampton, J. J. (2009). *Fundamentals of enterprise risk management: How top companies assess risk, manage exposure, and seize opportunity*: AMACOM Div American Mgmt Assn.
Hanson, S., Kashyap, A., & Stein, J. (2010). A macroprudential approach to financial regulation. *Chicago Booth Research Paper*(10-29).
Healy, P. M., & Palepu, K. G. (2001). Information asymmetry, corporate disclosure, and the capital markets: A review of the empirical disclosure literature. *Journal of accounting and economics, 31*(1), 405-440.
Herring, R., & Carmassi, J. (2008). The Structure of Cross-Sector Financial Supervision. *Financial Markets, Institutions & Instruments, 17*(1), 51-76.
Higgs, D. (2003). The Higgs Report: Review of the role and effectiveness of non-executive directors. *January,* http://www.bis.gov.uk/files/file23012.pdf.
Hilb, M. (2012). *New corporate governance: Successful board management tools*: Springer Science & Business Media.
Hilgartner, S. (1992). The social construction of risk objects: Or, how to pry open networks of risk. *Organizations, uncertainties, and risk*, 39-53.
Ho, V. (2012). Corporate Governance as Risk Regulation in China: A Comparative View of Risk Oversight, Risk Management, and Accountability. *Risk Management, and Accountability (August 28, 2012). University of Kansas School of Law Working Paper*.
Hölmstrom, B. (1979). Moral hazard and observability. *The Bell journal of economics*, 74-91.
Hood, C., Rothstein, H., & Baldwin, R. (2001). *The government of risk: Understanding risk regulation regimes*: Oxford University Press.

House of Commons. (2012). The FSA's report into the failure of RBS http://www.publications.parliament.uk/pa/cm201213/cmselect/cmtreasy/640/640.pdf.
HSBC. (2015). Governance: Board Committeess http://www.hsbc.com/investor-relations/governance/board-committees.
Huse, M. (2005). Accountability and creating accountability: A framework for exploring behavioural perspectives of corporate governance. *British Journal of Management, 16*(s1), S65-S79.
Huse, M. (2007). *Boards, governance and value creation: The human side of corporate governance*: Cambridge University Press.
Hutter, B., & Power, M. (2000). Risk management and business regulation. *Financial Times Mastering Risks*.
Hutter, B. M. (2001). Is enforced self-regulation a form of risk taking?: The case of railway health and safety. *International Journal of the Sociology of Law, 29*(4), 379-400.
IIA. (2013). Internal Audit Guidance: Effective Internal Audit in the Financial Services Sector. *July*.
International Corporate Governance Network, I. (2010). ICGN Corporate Risk Oversight Guidelines. *London, https://*http://www.icgn.org/files/icgn_main/pdfs/best_practice/icgn_cro_guidelines_(short).pdf.
IRM. (2015). Risk appetite and tolerance. *https://*http://www.theirm.org/knowledge-and-resources/thought-leadership/risk-appetite-and-tolerance/.
Jalilvand, A., & Malliaris, T. (2013). *Risk management and corporate governance*: Routledge.
Jensen, M., & Meckling, W. (1995). Specific and general knowledge and organizational structure.
Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of financial economics, 3*(4), 305-360.
Jorgensen, D. L. (1989). *Participant observation: A methodology for human studies* (Vol. 15): Sage.
Kahn, R. L., Wolfe, D. M., Quinn, R. P., Snoek, J. D., & Rosenthal, R. A. (1964). Organizational stress: Studies in role conflict and ambiguity.
Kaplan, R. S., & Atkinson, A. A. (1998). *Advanced management accounting* (Vol. 3): Prentice Hall Upper Saddle River, NJ.
Katz, D., & Kahn, R. L. (1978). The social psychology of organizations.
Kawulich, B. B. (2005). *Participant observation as a data collection method.* Paper presented at the Forum: Qualitative Social Research.
Keizer, H. (2010). Risk oversight is a 'team sport'. *Directors and Boards. Vol 34 (2)*.
Klausner, M., Munger, N., Munger, C., Black, B., & Cheffins, B. (2005). Outside directors' liability: have Worldcom and Enron changed the rules? *Stanford Lawyer, 71*, 36-39.
Koller, M. (2011). *Eaa: Life Insurance Risk Management Essentials*: Springer.
Koppell, J. G. (2005). Pathologies of accountability: ICANN and the challenge of "multiple accountabilities disorder". *Public Administration Review, 65*(1), 94-108.
KPMG. (2012). The Future of Compliance Compliance functions as strategic partners in the new regulatory world. (http://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/Documents/PDF/Advisory/future-of-compliance_web_Acc4.pdf).

KPMG. (2013a). Developing a strong risk appetite program. *https://*http://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/risk-appetite-v2.pdf.
KPMG. (2013b). The Three Lines of Defence. http://www.kpmg.com/RU/en/IssuesAndInsights/ArticlesPublications/Audit-Committee-Journal/Documents/The-three-lines-of-defence-en.pdf.
Kräussl, R. (2003). A critique on the proposed use of external sovereign credit ratings in Basel II.
Krippendorff, K. (Ed.). (1989). *Content Analysis*. New York, NY: Oxford University Press.
Kunz, A. H., & Pfaff, D. (2002). Agency theory, performance evaluation, and the hypothetical construct of intrinsic motivation. *Accounting, Organizations and Society, 27*(3), 275-295.
Laffont, & Tirole. (1993). A Theory of Incentives in Procurement and Regulation: MIT Press.
Lambert, R. A. (2006). Agency theory and management accounting. *Handbooks of Management Accounting Research, 1*, 247-268.
Langley, A. (1999). Strategies for theorizing from process data. *Academy of Management review, 24*(4), 691-710.
Leech, T. (2012). Risk Oversight: Is it "Broken"? What are the New Expectations? *EDPACS, 45*(4), 1-11.
Lin, L. (1995). Effectiveness of Outside Directors As a Corporate Governance Mechanism: Theories and Evidence. *Nw. UL Rev., 90*, 898.
Lodge, M. (2014). 10. Regulation in crisis: reputation, capacity and limitations. *Public Administration in the Context of Global Governance*, 96.
Loeb, M., & Magat, W. A. (1979). A decentralized method for utility regulation. *Journal of Law and Economics*, 399-404.
LSE. (2015). Research Ethics Policy and Procedures. http://www.lse.ac.uk/intranet/LSEServices/policies/pdfs/school/resEthPolPro.pdf.
Ludwig, E. A. (2012). Assessment of Dodd-Frank Financial Regulatory Reform: Strengths, Challenges, and Opportunities for a Stronger Regulatory System. *Yale J. on Reg., 29*, 181.
Lyons, S. (2012). Defending Our Stakeholders: Corporate Defence Management Explored. *The Business Continuity and Resiliency Journal, 1*(3), Q3.
Mace, M. L. (1971). Directors: Myth and reality.
McKinsey. (2010). Getting risk ownership right. *McKinsey working papers on risk, Number 23*
McKinsey. (2012). Enterprise risk management: What's different in the corporate world and why. *McKinsey working papers on risk, Number 40*.
McKinsey. (2014). Enterprise-risk-management practices: Where's the evidence? *McKinsey working papers on risk, Number 53*.
Mikes, A. (2011). From counting risk to making risk count: Boundary-work in risk management. *Accounting, Organizations and Society, 36*(4), 226-245.
Miller, K. D., & Waller, H. G. (2003). Scenarios, real options and integrated risk management. *Long range planning, 36*(1), 93-107.
Millstein, I. M., & MacAvoy, P. W. (1998). The active board of directors and performance of the large publicly traded corporation. *Columbia Law Review*, 1283-1322.
Morgan_Stanley. (2014a). Audit Committee Charter. http://www.morganstanley.com/about/company/governance/auditcc.html.

Morgan_Stanley. (2014b). Risk Committee Charter *https://*http://www.morganstanley.com/about/company/governance/pdf/rcchart.pdf?v=20140513.
Morgan_Stanley. (2014c). Risk Committee Charter. *https://*http://www.morganstanley.com/about/company/governance/pdf/rcchart.pdf?v=20140513.
Nestor. (2009). Governance in crisis: A comparative case study of six US investment banks. *April,* http://www.nestoradvisors.com/publications/governance-in-crisis-a-comparative-case-study-of-six-us-investment-banks/.
OECD. (2004). The principles of corporate governance.
OECD. (2010). CORPORATE GOVERNANCE AND THE FINANCIAL CRISIS. *February,* http://www.oecd.org/daf/ca/corporategovernanceprinciples/44679170.pdf.
Omarova, S. T. (2011). Wall Street as Community of Fate: Toward Financial Industry Self-Regulation. *University of Pennsylvania Law Review*, 411-492.
Peat, M. (1989). *Global Capital Markets 1989: A KPMG Survey*: Euromoney Publications PLC.
Per-Ardua. (2014). Chairman Survey. *Per Ardua Associates, July*.
Pettigrew, A. M. (1997). The double hurdles for management research. *Advancement in organizational behaviour: Essays in honour of DS Pugh*, 277-296.
Power, M. (1994). *The audit explosion*: Demos.
Power, M. (1999). *The audit society: Rituals of verification*: Oxford University Press.
Power, M. (2000). *The audit implosion: Regulating risk from the inside*: Icaew London.
Power, M. (2004). *The risk management of everything: Rethinking the politics of uncertainty*: Demos.
Power, M. (2007). Organized Uncertainty: Organizing a World of Risk Management: Oxford: Oxford University Press.
Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society, 34*(6), 849-855.
Power, M. (2012). Smart and Dumb Questions to Ask About Risk Management. *The Conference Board of Canada Risk Watch*.
Power, M. (2013). The apparatus of fraud risk. *Accounting, Organizations and Society, 38*(6), 525-543.
Power, M., Ashby, S., & Palermo, T. (2013). Risk Culture in Financial Organisations. *London School of Economics, London*.
PRA. (2014). Strengthening accountability in banking: a new regulatory framework for individuals. http://www.bankofengland.co.uk/pra/Documents/publications/cp/2014/cp1414.pdf.
PRA. (2015a). Assessing capital adequacy under Pillar 2. *January,* http://www.bankofengland.co.uk/pra/Documents/publications/cp/2015/pillar2/cp115.pdf.
PRA. (2015b). Consultation Paper: "Corporate governance: Board responsibilities" - CP18/15. http://www.bankofengland.co.uk/pra/Pages/publications/cp/2015/cp1815.aspx.
PRA. (2015c). Consultation Paper: Corporate governance - Board responsibilities. http://www.bankofengland.co.uk/pra/Documents/publications/cp/2015/cp1815.pdf, *May*.
PRA. (2015d). Strengthening Acocuntability. http://www.bankofengland.co.uk/pra/Pages/supervision/strengtheningacc/default.aspx, *July*.

Prager, J. (2013). The financial crisis of 2007/8: Misaligned incentives, bank mismanagement, and troubling policy implications. *Economics, Management, and Financial Markets*(2), 11-56.
Protiviti. (2012). Risk Culture: Guidance from the Institute of Risk Management. *August*(http://www.theirm.org/documents/RiskCultureWorkingDraftJuly2012.pdf - page=49).
PwC. (2013). The Insurance Industry in 2013 - Top Issues. http://www.pwc.com/us/en/insurance/publications/assets/pwc-top-insurance-industry-issues-2013.pdf.
Pwc. (2015). Effective Internal Audit. http://www.pwc.ru/en/internal-audit-services/committee-member-shareholder.jhtml.
RIIF. (1927). The Chatham House Rule. 2015_Dec_Whole.docx.
RiskDynamics. (2014). Risk Appetite Framework. http://www.riskdynamics.eu/Portals/156514/images/Risk Appetite Framework.jpg.
Roberts, J., McNulty, T., & Stiles, P. (2005). Beyond agency conceptions of the work of the non-executive director: Creating accountability in the boardroom. *British Journal of Management, 16*(s1), S5-S26.
Roberts, J., & Stiles, P. (1999). The Relationship between Chairmen and Chief Executives: Competitive or Complementary Roles? *Long Range Planning, 32*(1), 36-48.
Ross, S. (1973). The economic theory of agency: the principals problem, 63 AER P&P. *S. 134ff*.
Salamon, L. M. (2002). *The tools of government: A guide to the new governance*: Oxford University Press.
Salz, A. S. (2013). Salz Review: An Independent Review of Barclays' Business Practices *April*(http://www.salzreview.co.uk).
Sass, T. R. (1984). Economics of information intermediaries.
Sauder, M., & Espeland, W. N. (2009). The discipline of rankings: Tight coupling and organizational change. *American Sociological Review, 74*(1), 63-82.
Schuffham, M. (2015). "UK bankers face 'reversed burden of proof' under new rules", *Reuters*.
Schulz, W., & Held, T. (2004). *Regulated Self-Regulation as a Form of Modern Government: an analysis of case studies from media and telecommunications law*: Indiana University Press.
SEC, S. a. E. C. (2010). Proxy disclosure enhancements. *February,* http://www.sec.gov/rules/final/2009/33-9089.pdf.
Shapiro, S. P. (2005). Agency theory. *Annual review of sociology*, 263-284.
Simons, R. (1990). The role of management control systems in creating competitive advantage: new perspectives. *Accounting, organizations and society, 15*(1), 127-143.
Sinclair, D. (1997). Self-regulation versus command and control? Beyond false dichotomies. *Law & Policy, 19*(4), 529-559.
Smith, A. (1776). An inquiry into the nature and causes ofthe wealth of nations. *London: George Routledge and Sons*.
Spira, L. F., & Bender, R. (2004). Compare and contrast: Perspectives on board committees. *Corporate Governance: An International Review, 12*(4), 489-499.
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.
Spira, L. F., & Page, M. (2010). Regulation by disclosure: the case of internal control. *Journal of Management & Governance, 14*(4), 409-433.

Spradley, J. P. (1980). Participant observation.
Stake, R. E. (2013). Qualitative Research and Case Study. *Silpakorn Educational Research Journal, 3*(1-2), 7-13.
Steffee, S. (2011). Aligning risk with strategy. *September, Directorship 34/7*.
Stempel, G. H. (1952). Sample size for classifying subject matter in dailies. *Journalism Quarterly, 29*(2), 333-334.
Sweeting, P. (2011). *Financial enterprise risk management* (Vol. 1): Cambridge University Press.
Treadway, J. C. (1987). *Report of the national commission on fraudulent financial reporting*: The Treadway Commission.
UK_Parliament. (2013). Parliamentary Commission on Banking Standards Report *June,* http://www.parliament.uk/business/committees/committees-a-z/joint-select/professional-standards-in-the-banking-industry/publications/.
Vaivio, J. (2008). Qualitative management accounting research: rationale, pitfalls and potential. *Qualitative Research in Accounting & Management, 5*(1), 64-86.
Wachtell, L. (2015). July Memo. *Risk Management and the Board of Directors*.
Walker, D. (2009). Review of Corporate Governance in UK Banks and other Financial Industry Entities – Final Recommendations. *November*.
Walsh, D. (1998). Doing ethnography. *Researching society and culture*, 217-232.
Ward, R. D. (2003). *Saving the corporate board: Why boards fail and how to fix them*: John Wiley & Sons.
Williams, A. P., & Taylor, J. A. (2013). Resolving accountability ambiguity in nonprofit organizations. *Voluntas: International Journal of Voluntary and Nonprofit Organizations, 24*(3), 559-580.
WSJ. (2014). RBS on What Went Wrong in the European Stress Tests, *Wall Street Journal*.
Yellen, J. L. (2011). Macroprudential supervision and monetary policy in the post-crisis world. *Business Economics, 46*(1), 3-12.
Young, M. (2010). The Board And Risk Management. *Corporate Board, 31 (183)*.
Zietsma, C., & Lawrence, T. B. (2010). Institutional work in the transformation of an organizational field: The interplay of boundary work and practice work. *Administrative Science Quarterly, 55*(2), 189-221.
ZYen. (2015). The Global Financial Centres Index 15. *March*.