In Search of explanations for risk management failures

Margaret Woods[a]

Christopher Humphrey[b]

Chu Yeong Lim[c]

[a] Aston Business School, Aston University. [b] Manchester Business School, The University of Manchester. [c] Singapore Management University. Corresponding author. Email: m.woods@aston.ac.uk

This paper is an early draft and should not be quoted without the authors' written permission. Chu Yeong Lim gratefully acknowledges research funding from the European Community's Seventh Framework Programme FP7-PEOPLE-ITN-2008 under grant agreement number PITN-GA-2009-237984 and the Singapore Management University. We thank Georgios Kominis and participants at the 2011 ENROAC conference for their helpful comments.

In search of explanations for risk management failures

ABSTRACT

The global financial crisis has generated calls for better risk management to prevent the risk exposures and strategic management failings in recent years. Criticisms of risk management and measurement have been made. This conceptual paper seeks to add to this existing literature by arguing that risk management is not just a matter of models or methodologies but also their application in practice. We build on the work of Power by questioning whether the problem with Enterprise Risk Management (ERM) is one of implementation rather than design. Using examples from the financial services sector we demonstrate how the operation of risk management and control systems is fundamentally dependent upon the effective co-ordination of interlinked layers of risk defences. Poor co-ordination can lead to risk imbalances and control problems and when multiple imbalances interact and occur simultaneously, there is risk of a fundamental failure of the risk management system.

Analysing the dynamics of the internal and external relationships between risk managers, operational managers, the Board of Directors, regulators, rating agencies and stakeholders we identify three areas – risk architecture, information flows and 'culture' which together serve to create misunderstandings and alternative perspectives about risk management that is not consistent with the ERM model, creating imbalances that undermine the stability of the control system. We conclude that ERM implementation is hampered by the cumulative eefect of failures to collaborate both within and outside the organization.

In search of explanations for risk management failures

"Among the illusions with which have invested our civilization is an absolute belief that the solutions to our problems must be a more determined application of rationally organized expertise… The reality is that our problems are largely the product of that application."

(Saul, 1993)

Introduction

Enterprise wide or holistic risk management, most commonly referred to as Enterprise Risk Management (ERM) has been growing in popularity since the mid 1990s. ERM is characterised as a system through which an organization seeks to understand and consolidate its exposure to a wide range of risks, and manage them through an integrated process (Culp, 2002). In guidance on the adoption of ISO 31000 (Risk Management: Principles and Guidelines) and the implementation of a structured approach to ERM, it is suggested that: "An enterprise-wide approach to risk management enables an organisation to consider the potential impact of all types of risks on all processes, activities, stakeholders, products and services. Implementing a comprehensive approach will result in an organisation benefiting from what is often referred to as the 'upside of risk'" (p.2,AIRMIC, 2010).

Dickinson (2001) argues that ERM emerged as a response to calls for better corporate governance following a series of high profile corporate failures such as Polly Peck in 1990, BCCI in 1991 and the Maxwell Group pensions affair of 1991. At that time risk was beginning to play a central role in finance theory, with the latter also placing increasing emphasis on value based management (Dickinson, 2001). Consequently, ERM was seen as offering a mechanism by which shareholder value could be potentially increased. Power (2005) supports this view of ERM's origins and argues that it has given rise to the idea that internal controls form the foundation of a "good organization".

The 1990s have been described as a decade characterised by an "explosion" in popularity of risk management (Culp,2002) , but it was also one marked by the collapse of Barings (1995) and the Procter and Gamble/ Bankers' Trust case (1996). The new millennium began with further major financial scandals including Enron, Global Crossing and Worldcom in 2001 and 2002. In response, the profile of risk management was raised still further with the passing of the Sarbanes Oxley Act (SOX) in 2003 and the issue by the Committee of Sponsoring Organizations (COSO) of a formal framework for enterprise risk management (COSO, 2004). Nonetheless, this growing array of risk management guidance and regulation failed to prevent the global financial crisis that began in 2007 and some observers now suggest that risk management in its current form is almost dysfunctional.

Criticism of risk management and measurement, and the search for explanations for its apparent failure has taken a number of forms. In recent years within finance there has been widespread adoption of specialised risk measurement tools such as the Blacks Scholes model for option pricing (Millo and Mackenzie, 2009) but at the same time much has been written about the limitations of the quantitative models on which much financial risk management depends [see for example, Rebonato (2007), Taleb (2007) and Tett (2009)].

More broadly, Power (2009) suggests that ERM as a system is fundamentally flawed. He demonstrates both its failings and its fragile foundation by pointing to the obsession with measurement and the emergence of a compliance and legitimacy culture designed to avoid liability. He also suggests that ERM systems are more about placing boundaries around risk management rather than managing risk and confronting the complexities of organizational life (Power, 2009).

In this paper we seek to add to this existing literature by arguing that risk management is not just a matter of models or methodologies but also about their application in practice. We build on the work of Power by questioning whether the problem with ERM is one of implementation rather than design.

Culp (2002) regards ERM as a process which aims to increase firm value by integrating a company's strategic and financial decisions with its risk management decisions. The key word idea here is *integration*. How does an organization ensure that strategic and operational decision making is referenced back to a desired level of risk taking? In practice, how do firms adopt the approach suggested by Warren Buffet in which "They accept only those risks that they are able to properly evaluate (staying within their circle of competence) and that, after they have evaluated all relevant factors including remote loss scenarios, carry the expectancy of profit" (Buffett,2001)?

There is growing evidence within both the academic and practitioner literature of the extent of ERM adoption (Gupta,2006; Deloitte,2011) and a number of studies have begun to appear which look at risk management systems within individual institutions (Arena et al, 2010; Mikes, 2009; Woods, 2009; Woods 2011). There is, however, a lack of critical empirical research looking at the social and political context of ERM and the resulting problems posed for its implementation.

This paper is premised on the belief that much more attention needs to be devoted to the practical intricacies and lived experiences of risk management systems (Humphrey et. al., 2009).Risk management practice includes a human dimension and yet this is an area that has so far gained little attention within the risk management literature. The central aim of this paper is to demonstrate how the operation of risk management and control systems is fundamentally dependent upon the effective co-ordination of interlinked layers of risk defences. Poor co-ordination can lead to risk imbalances and control problems and when multiple imbalances occur simultaneously and interact, there is a fundamental failure of the risk management system.

We adapt and apply Reason's (2000) Swiss Cheese model of system failure and "vulnerable systems syndrome" (Reason et al 2001) to explain how risk management practice can fail even when seemingly sophisticated control systems are in place. The Swiss Cheese model has been extensively applied in the fields of healthcare practice and safety engineering and we apply it to the financial services sector to demonstrate how risk imbalances can penetrate and undermine formalised risk management defences and cause localised or organisation wide control failures.

Within the financial services sector, risk management takes the form of the building of external defences in the form of both global and national regulations. Internal defences traditionally take the form of the so called "three lines of defence model" which portrays three parties as being core to good risk management. The first line of defence is the operational staff within the business who take front line responsibility for assessing, measuring and monitoring risks. Second line defence comes from the risk management function and the third line of defence is internal audit whose role is to provide board level assurance on the effectiveness of internal controls. The three lines of defence model is the one preferred by the UK regulator the FSA.

In this paper we analyse the dynamics of the internal and external relationships between risk managers, operational managers, the Board of Directors, regulators, rating agencies and stakeholders and identify three areas – risk architecture, information flows and 'culture' which together serve to create a variety of misunderstandings and alternative perspectives amongst the various actors. The resulting behaviour is inconsistent with the ERM model but, more fundamentally, increases the potential for risk management failure. We conclude that ERM implementation is hampered by failures of collaboration both within and outside the organization, which serve to threaten the validity of the overall risk management system. This finding supports the opinion of the Walker Review into corporate governance in financial services in the UK that "Good corporate governance overall depends critically on the abilities and experience of individuals and the effectiveness of their collaboration in the enterprise. Despite the need for hard rules in some areas, this will not be assured by overly-specific prescription that generates box-ticking conformity." (Walker Review 2009: 7).

The rest of the paper is structured as follows. The next section incorporates a literature review which presents the case for ERM as a set of structures or frameworks which are based on the assumption that risks can be identified, measured and managed. It also highlights the growing concern that organisations are installing ERM systems which appear to be poorly embedded, resulting in a loss of emphasis on the core objective of improving corporate performance and value, and suggesting the existence of a mismatch between the theoretical model of ERM and ERM in practice. This mismatch forms the primary justification for our paper. Section 3 defines the overall concept of risk imbalance and summarises the framework used in the paper to analyse these imbalances. Section 4 defines each type of risk imbalance and illustrates it with an empirical example(s) to show how it may lead to misunderstandings about risk and a lack of coherence in the implementation of ERM. A discussion of the implications of these imbalances then leads us to the conclusion that ERM is a highly complex practice, but also one that currently places excessive emphasis on the structural elements of the process and too little on the communication and information components. The result is that evidence of the existence of ERM labelled structures within an organization offers no guarantee that they have been implemented, embedded or will prove effective when a crisis strikes.

Theory versus Practice in ERM

The COSO framework is now regarded as the worldwide template for best practice in ERM (Power, 2007) and its significance is reflected in its incorporation into ISO 31000, the most recent international standard on risk management (ISO, 2009). Supporters of ERM argue that the rationale for its adoption is a belief that risk management can help in protecting and potentially increasing shareholder value. It is argued that ERM can both reduce the downside

of risks whilst simultaneously helping to inform decision making and aid the efficient internal allocation of capital (Hoyt and Liebenberg, 2011). Most importantly, good risk management can raise external perceptions of an organization, and so help to protect its reputation (AIRMIC, 2010), which is regarded as a valuable asset.

Whilst there is strong support in the practitioner literature for the idea that risk management can enhance shareholder value (IFAC/CIMA, 2002; PwC, 2007) there is a lack of research evidence on the impact of ERM on firm value (Hoyt and Liebenberg, 2011). In a review paper, Smithson and Simkins (2005) found evidence that the use of derivatives for risk management purposes by both financial and non financial firms served to reduce the sensitivity of equity returns to financial risks. Furthermore, using Tobin's Q as a proxy for a firm's value, they concluded that there is a positive relationship between risk management and firm value. The limitation of Smithson and Simkin's survey, however, is that it only found research results relating to the use of very specific, derivative based, forms of financial risk management. The survey thus offers no insights into the possible value impact of a more broadly based holistic risk management system such as ERM. Using a longitudinal sample of 275 publicly listed US insurance companies, Hoyt and Liebenberg (2011) found some support for the contention that ERM enhances firm value. Their results indicate that, after controlling for other value determinants and potential endogeneity bias, insurers engaged in ERM are valued roughly 20 percent higher than other insurers. In the light of the banking crisis, however, which saw huge falls in equity prices, much more research into the effect of ERM on shareholder value is required.

COSO (2004) defines ERM as "a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." Implicit in this definition is the idea that risks can be managed through the application of rationally organized expertise, echoing Beck's suggestion that "the social perceptions of risks remain dependent on scientific rationality" (Beck, 1992:p.59). ERM's codification serves to rationalise risk management processes under the headings of risk identification, assessment, response, reporting, control and monitoring. The belief that ERM will enable a wide range of risks to be identified, measured and managed implies that risk is a distinct object – a thing apart- that can be associated with specific sources and/or outcomes. We can identify a risk, specify its cause(s) and consequence(s) and respond so that the exposure to risk stays within the desired appetite. Furthermore, ERM assumes a single organizational risk appetite and entity boundary on the risks that are to be managed (Martin & Power, 2007).

Young (2001) argues that this objectification of risk leads on to the idea that risk management is a taken for granted element of a well run business. It is the perception that risk management and internal controls are intrinsically 'good' which predicates the ongoing push for greater regulation of risk taking and results in risk management systems that are shaped by the regulatory environment of Sarbanes Oxley, Basel II and broader corporate governance guidance (Woods,2011). The rational, theoretical view of risk management that is embodied within ERM is thus one which is system and process oriented but simultaneously fails to acknowledge the behavioural and power dimensions that influence risk management practice. Power suggests, "the challenge is to expand processes which support interaction and dialogue and de-emphasise due process" (Power, 2009, p.852), but as already indicated, there

has been little research to date into either why this is not being done, or how it might be achieved.

The continuing recurrence of apparent problems of risk management in the twenty years since ERM began to become popular raises the fundamental question of what exactly is being managed by ERM based systems. Is it, as claimed, the holistic collection of risks faced by an entity, or does ERM represent an obsession with measurement and compliance aimed at ensuring organizational legitimacy and avoidance of liability? Does ERM really represent the risk management of nothing (Power, 2009)? We suggest that ERM is an example of the "fallacy of misplaced concreteness" [1], where repetition of the mantra of holistic risk management has led to an unquestioning adherence to an underlying dogma which remains as yet largely unproven. The result is a mismatch between the theory and practice of enterprise risk management, which we seek to explain in terms of risk imbalances.

In the last five years companies such as Lehman Brothers, AIG and Merrill Lynch have all run into financial troubles, despite having risk management systems which were variations of ERM. It is perhaps not surprising then that politicians (G20, 2008; OECD, 2009), regulators (Senior Supervisors Group,2009; Committee of European Banking Supervisors, 2010; Basel Committee,2010) and practitioners (KPMG,2011; PwC,2012) are now questioning the day to day practice of risk management and presenting the case for change. Some companies are even beginning to question the return on spending they are getting from ERM frameworks, given the level of protection they are gaining from them (PwC, 2012).

Central to the ongoing criticisms is the suggestion that ERM (or its equivalent) is not sufficiently "embedded". Power (2009) notes that whilst the concept of embedding appears to be an ERM imperative, it remains poorly articulated and hence elusive. ISO 31000, based on the COSO framework, interprets the term embedded as meaning that risk management thinking and processes are integral to ordinary business activities, so that operational staff recognise and are held responsible for risk management. In such a situation, risk management moves beyond a specially designated unit or function and out into the business as a whole. Responsibility for ensuring that risk management is embedded into all processes and activities rests firmly with the Board of Directors (AIRMIC, 2010).

Implicit in the suggestion that responsibility for embedding risk management across the organization rests with the Board are the twin ideas that Board members are both committed to a holistic approach to risk management and also "have substantially complete access to, and understanding of, information about all the important risks faced by their organisations" (Airmic/Cass, 2011, p. 4). The inaccuracy of this assumption, even within highly respected companies, is clearly evidenced in the "Roads to Ruin" report by Cass Business School (Airmic/Cass, 2011), which analyses and pinpoints lessons from eighteen case studies of major risk management failure, including AIG, Enron, Northern Rock and Cadbury Schweppes. PwC (2012) confirms and extends this view in suggesting that not only do the boards of big organizations often not understand the risks their businesses are running, but are also unaware of the knock on effects of risks interacting and spreading across a range of areas. KPMG (2011) re-iterate the concerns about the extent of top level commitment and support for risk management in companies, and note that whilst regulatory compliance

[1] See Whitehead (1925) for a detailed explanation of this concept which has been widely used in the economics literature.

remains a priority for many, the softer issue of embedding risk into the organizational culture is "not getting the attention it deserves" (KPMG,2011,p.6).

We argue that the apparent failure by some Boards of Directors to engage with, understand and embed holistic style risk management systems such as ERM reflects a problem of risk imbalance. That is, a situation which gives rise to inequalities between risk actors in terms of the level of information and understanding about the control environment, organizational risk appetite and exposures, and/or the power to influence both operational and strategic decisions in the light of such information. The term risk actor refers to any party with an interest in the risks being taken by an organization, and their management. The next section establishes a framework for the identification and analysis of risk imbalances and demonstrates that where they are interdependent then their impact is potentially cumulative and catastrophic.

A Risk Imbalance Framework

"Internal control is most effective when controls are built into the entity's infrastructure and are a part of the essence of the enterprise."(COSO 2004, p.3).

The basic concept

A risk imbalance implies that the risk management system/process is not working effectively and the relevant controls are not permeating the organisation as suggested in the above quote. A risk imbalance may originate anywhere in the internal control system and our proposed framework suggests a range of potential categories and forms of imbalance.

The framework identifies three types of risk imbalances - two structural and one which is information based. We also suggest that these imbalances may originate either inside or outside an organisation. The two structural categories of risk imbalance are the control environment and the risk architecture. These are structural insofar as they relate to the mechanisms used to form the overall control environment and the day to day operation of the risk management system respectively. An information risk imbalance is defined as reflecting differences in understanding between risk actors about risk exposures, potential impacts and control effectiveness.

Table 1 shows a three by two matrix denoting the three categories of imbalance identified above.

INSERT TABLE 1 ABOUT HERE

An explanation of each category, including illustrative examples, is detailed below. We confine our illustrative examples to the financial services sector, but further research could usefully investigate the framework's wider applicability to other industry sectors.

The Control Environment

COSO (2011, para.23) defines the control environment as "the set of standards, structures and processes that provide the basis for internal control across the organization" and affirms that it is the Board of Directors who set the 'tone at the top' in terms of ethical stance, risk appetite and attitude to risk management. Board responsibility for control of risks is extended still further in the UK's corporate governance code which states that directors are

also responsible for determining the nature and extent of the significant risks the Board is willing to take in pursuit of its strategy (FRC, 2011).

The OECD's Principles of Corporate Governance (OECD, 2004) clearly state that one of the board's key functions is "reviewing and guiding.... risk policy" (Principle VI D.1) and more specifically "Ensuring the integrity of the corporation's accounting and financial reporting systems, including the independent audit, and that appropriate systems of control are in place, in particular, systems for risk management, financial and operational control, and compliance with the law and relevant standards" (Principle VI.D.7). Ensuring the integrity of the systems of control requires that the board instigates appropriate systems of oversight by senior management whilst also specifying the lines of responsibility and accountability for risk (OECD, 2009). Most importantly, the oversight role should relate to future events and the potential risks posed by a given strategy, rather than simply a historical review of risk management performance (OECD,2009).

Imbalance in the control environment may therefore be caused by senior management failures to fulfil their responsibilities in relation to risk management. If Board members do not make it clear that they are closely involved in managing risks and engage in very limited oversight of the ERM systems, then there is a clear danger that risks will spiral out of control. Earlier in the paper we provided examples of general comment about the apparent lack of active board involvement in risk management, but more detailed illustrations confirm the idea that board level attitudes can create a potential risk imbalance.

In their report "Roads to Ruin" (Airmic/Cass, 2011) the authors identify several key factors at board of director level that can nurture risk management failure. These include inadequate board leadership in establishing a risk aware culture, the inability of non executive-directors to exercise control, inadequate skills, and a failure by the Board to understand and engage with the risks associated with the business. These criticisms fall into two interlinked categories – poor leadership and engagement and lack of skills/knowledge. Referencing Table 1, this form of risk imbalance is internal to the organisation and takes the form of a weak "tone at the top".

A report by the Institute of International Finance (2008) concluded that the financial crisis raised serious questions about the ability of certain boards to understand and monitor their business and provide senior management oversight. Seven of the ten directors of Lehman Brothers were retired CEO's of non financial firms (Magnan & Markarian 2011) and only one had current experience of the financial sector (OECD, 2009). Similarly, two-thirds of directors at eight major US financial institutions were found to have no banking experience at all (Guerrara & Thai-Larsen, 2008). Evidence of imbalances caused by the directors' lack of necessary knowledge or experience is widespread. Lapido et al (2008) found in interviews with major European banks that the majority of banks acknowledged that board members were broadly rather than extremely knowledgeable about their bank's risk measurement methodologies. Worryingly, the imbalances seem to be two tiered in that there is a lack of knowledge of the banking industry that is further compounded by a limited understanding of risk management and measurement tools.

Table 1 also indicates that further imbalance is nurtured by the executive remuneration systems in the banking sector, which have been blamed for encouraging senior management to focus on growth of turnover or returns on equity at the expense of risk management. The Turner Review (FSA, 2009: 82) notes that "there is a strong prima facie case that

inappropriate incentive structures played a role in encouraging behaviour which contributed to the financial crisis." Erkens et al (2009) notes the pressures imposed by institutional investors for short term oriented bonus plans for senior executives and similarly Livne & Markarian (2010) and Chesney et al (2010) argue that CEO bonus systems and other executive compensation plans may have served to increase firms' risk taking. In our framework, such remuneration systems, particularly for board members, constitute a potential imbalance by creating the scope for management to engage in risk taking that does not match the broader organisational risk appetite.

The internal control environment is subject to external influences, most obviously in the form of regulation and these influences may create imbalances in perception between external and internal risk actors about risk identification, measurement and management. Evidence suggests that ERM has been heavily influenced by regulation, most notably the COSO 2004 framework, Basel 2 and the Sarbanes Oxley Act in the United States (Martin & Power, 2007). Martin & Power (2007) argue that COSO 2004 serves as an "idealised blueprint" for the risk management process that emphasises high level accountability via regulatory compliance at the expense of operational risk management. Compliance with regulatory requirements may, in the language of institutional theory, serve to legitimise an organisation's position, but it does not mean that risk management is embedded and an integral part of the culture. As Magnan and Markarian (p.224) observe "structures might look good on paper" but "form should never be confused with function." A good example of this is the fact that Lehman Brothers had a risk committee which was a sub-committee of the board, but they only met twice a year (Caplain, 2008) and unsurprisingly their potential effectiveness in managing risk was strictly limited.

Observed failures of regulation and particularly the use of so called "light touch" approaches in the area of financial services suggest an imbalance between what regulators think they see and what may actually be happening inside an organisation in relation to risk management. Inadequacies in the supervisory approach were first raised in relation to the failure of Northern Rock (FSA, 2008) and again by the Turner Review (2009). The FSA now acknowledges that large, systemically important banks were not allocated the necessary supervisory resources and there was "inadequate focus on the core prudential risk areas of capital adequacy, liquidity, asset quality, balance sheet composition, and leverage" (FSA, 2011, p.255). In their report on the failure of the Royal Bank of Scotland, for example, the Financial Services Authority admitted that whilst it had identified a number of potential areas of concern within the bank, "the degree of supervisory intensity applied to these issues" was less than they would now consider appropriate (FSA, 2011, p.253). In other words there is evidence of an imbalance between the regulator's view of risk exposure and management in large institutions and the internal reality within that bank. Evidence in support of this view is reinforced by regulatory delays in identifying the manipulation of LIBOR in the UK and HSBC's breach of US regulations on money laundering in relation to the use of funds originating in Iran.

The arguments outlined above, and the associated examples demonstrate that a number of elements within both the internal and external control environment may create risk imbalances that could result in risk management failures. We now look at the second category of risk imbalances identified in Table 1 – the risk architecture of an organisation.

Risk Architecture

The control system serves to define an organisation's 'tone' in relation to risk management, or what is sometimes termed the 'risk culture', but in practice that culture needs to be translated into structures and process that support the risk management/ERM process. The risk architecture performs this function by specifying the roles, responsibilities, communication and risk reporting structure (AIRMIC, 2010). A variety of committees and individuals may hold responsibility for risk management processes and the risk architecture defines those responsibilities and the systems to be used internally for the communication of risk information. The guidelines within ISO 31000 suggest that the architecture also includes structures to ensure monitoring and review of the roles and communication systems, to ensure that the framework is continually redesigned and improved over time. The control environment and the risk architecture are therefore closely linked even though one relates largely to an organisational mindset, whilst the architecture relates to structures. It is perhaps not surprising therefore, that COSO has been criticized for a framework that is confusing in the way that it mixes framework specification with process (Marks, 2011).

Establishing lines of responsibility for risk and defining the necessary structures to support those responsibilities is challenging, and one noticeable trend over the last decade has been a growing tendency for the lines of responsibility and roles within the risk architecture to be held by risk "professionals". Banks have responded to regulatory requirements/recommendations to appoint a Chief Risk Officer (CRO) and Table 2 reveals that, according to the 2010 annual reports, six of the world's largest banks all have Chief Risk Officers, but in only one of them is the CRO a main board member.

Insert Table 2 about here

In practice, the effectiveness of the CRO is heavily dependent upon the power they are granted to contribute to and influence both strategic and operational decision making. It is also noticeable from Table 2 that there is some variation in practice over the person to whom the CRO reports. In the US banks, the CRO reports directly to the CEO and in Deutsche Bank the position is similar with reporting to the Chair of the Supervisory Board. In the UK, however, each bank is different, and the reporting line in HSBC not clearly identified in the annual report. This variation is interesting given that the Walker Review (2009) recommended that the CRO report directly to either the CEO or Finance Director and the Board Risk Committee. Internal reporting lines on matters of risk are important to ensuring both the independence and level of influence of the CRO, and their importance was emphasised in the Walker Review (2009, p.98) in its statement that "the CRO would be expected to be in a position to assess, *independently of the executive* in individual business units, and with due regard to materiality, whether a proposed product launch or the pricing of risk in a particular transaction is consistent with the risk tolerance determined by the risk committee and board, and should be *able to exercise a power of veto* where necessary."

It follows that the appointment of a CRO does not automatically imply that risks are better managed and Table 1 suggests that such 'professionalization' may actually create risk imbalances by working to place artificial boundaries around risk domains and reducing Board knowledge of risk exposures and management tools. The evidence in support of this is as follows.

There is little evidence, to date, to confirm that a CRO appointment adds value for an organisation (Beasley et al, 2007). As noted above, the professionalization of risk can be seen as taking the pressure of the Board because risk management can now be left to the "experts",

leaving the directors to focus on strategic issues. At the same time, if the control environment is one in which the CRO is not invited to engage in risk dialogues with Board members on issues of strategy, or one where the CRO's views go unheeded if they are considered contentious then risk may not be well understood at the top of the organization.

The American International Group (AIG) had an ERM system in place, with a chief risk officer responsible for the ERM but this still that did not prevent AIG (specifically its financial products unit) from taking excessive risks (Asher and Heaser, 2008; Wacek, 2011). In particular, risk management was applied selectively as AIG management allowed its financial products unit to limit the access of senior risk officers (Wheelhouse Advisors, 2009; Boyls, 2010). In other words, there were clear risk imbalances within the risk architecture of AIG that were not properly managed.

The case of Paul Moore, the former head of regulatory risk at HBOS similarly suggests that the power of the CRO can be severely restricted in practice. In evidence given to the Treasury Committee of the House of Commons in 2009, Moore revealed that he had raised major concerns about actual or potential breaches of regulatory rules with the bank's Chief Financial Officer, the group audit committee and the Board (Dewing, 2012) but to no avail. He concluded that the breaches were caused by a lack of separation of duties between executive staff and the functions responsible for their oversight, including risk, compliance and internal audit, non-executive directors, external auditors and the FSA. (TC, 2009). The failure to segregate oversight from executive responsibility was compounded by an imbalance in the power exercised by the two parties, with the control function being the weaker party.

Given that the responsibilities and powers granted to the CRO and their staff are laid down in the risk architecture, we begin to see that problems in the control system or 'tone at the top' can result in the creation of imbalances in the risk architecture. The framework of imbalances is interlinked, and we discuss this in more detail in the next section of the paper.

The professionalization of risk has been further enhanced by the ways the Basel capital regulations are implemented, through the categorisation of banking risks into market, credit, liquidity and now operational risks. While the Basel regulations are intended to encourage the holistic summarizing the banks' risks via an overall capital requirement, in practice the banks structure their control environment around risk silos, which are critical for regulatory reporting purposes.

The appointment of a head of risk for each silo means that responsibility for its management can be delegated and the need for internal oversight may be perceived to be reduced. In practice, however, the silos can interact and lead to increased aggregate risk. When the sum of the whole is more than the sum of the parts, the organisation wide view is only really feasible at a more senior, effectively Board level. In his study of failures in the insurance sector, Ashby (2003) notes that holistically informed board oversight is critical to preventing failure. For example, credit insurers who invested in commercial property in the recession of the 1990s suffered from both falls in asset values but simultaneous losses from the resulting credit failures. The "experts" managing the assets could argue that independently they were doing a "good" job, but it was the combined impact that was lethal.

When banks implement the Basel regulations via a silo based approach to risk management in contrast to the COSO and ISO 31000 emphasis on a holistic ERM style of approach there is clearly a mismatch between theory and practice. In other words, there is some imbalance in

the thinking about risk management that arise from the rules of different regulatory bodies, and these mixed messages can be expected to cause at least some confusion within organizations. Which approach should be prioritised? Is compliance with Basle intrinsically contradictory to compliance with COSO and if not then how can they be merged? In Table 1 we categorise these issues as an external imbalance in the risk architecture, but it is also useful to recognise that this imbalance is potentially aggravated by a compliance focused approach to risk management. If compliance requires that credit, market and liquidity risks are managed and reported separately to regulators then the oversight of cross cutting risks may be imperilled as the big picture is missed.

The compliance focused culture is further nurtured by the ever growing list of regulations to be followed. A recent report (Thomson Reuters, 2012) noted that there were a total of 14,215 regulatory announcements made in 2011, equivalent to 60 per working day. The volume of announcements has grown steadily since 2008 and companies face a massive challenge to ensure ongoing compliance whilst releasing funds for use elsewhere in the business. This point is well illustrated by the recent case of Morgan Stanley's revisions to its Value at Risk model following its $7 billion trading loss is an example of such challenge. The model was revised to increase the weighting given to one year historical data, instead of the four year data used in the previous model (Alloway, 2012). The result was a fall in the bank's VaR from $82m to $63m in the most recent quarter, enabling Morgan Stanley to reduce its regulatory capital ratios and appear less risky to the market. This type of action is classified in Table 1 as an external imbalance in the risk architecture arising from regulations which encourage regulatory arbitrage.

The last example of an external imbalance in the risk architecture relates to the role and power of the credit rating agencies. At the height of the financial crisis the market lost faith in the credit ratings process when the three major rating agencies (Standard & Poor's, Moody's and Fitch) re-ran their models in July 2007 after the failure of two Bearn Stearns hedge funds. The agencies subsequently down-graded eight notches of ratings to junk status – equal to 20% of the CDOs issued in 2006-2007. The credit rating practices and their models were effectively the key intermediaries that inter-connected market participants (Roberts, 2009) and the ratings were a core part of CDO valuations. High ratings meant high prices but the agencies came under fire from both politicians and investors for their role in generating supposedly inaccurate risk classifications for such securities (Graybow, 2008). In terms of our framework, the credit rating agencies created a risk imbalance that camouflaged actual levels of risk exposures and ultimately led to massive write downs of bank assets.

Information and/or understanding of risks

Risk identification establishes the exposure of an organisation to risk and uncertainty and is complemented by risk analysis which can be used to produce a risk profile that rates the significance of each risk and facilitates the prioritisation of risk management efforts. In practice, however, risks will be identified and analysed by operational staff and there is potential for a risk imbalance to arise if there are differences between the perceptions of the operational staff, internal controllers, risk managers and/or the Board of Directors' in respect of any of the following: the organisational risk appetite, current risk exposure, and the effectiveness of risk monitoring and management tools. Such imbalances are categorised in Table 1 under the heading of information and/or understanding of risks.

The problems of differences in understanding between headquarters and operational staff in banking is blamed in part by Wahlstrom (2009) on the recruitment of relatively young staff to HQ who lack long term experience of the industry. These young risk specialists are expert at

theoretical modelling but have little or no practical experience. One of Wahlstrom's interviewees, the head of internal control in a Swedish bank observed that this resulted in a belief that risk measurement could solve all problems and risk staff being insufficiently critical of the numbers. The situation was compounded by what some of his interviewees called the "excessive complexity" of the Basel regulations. Such complexity creates challenges for the Board of Directors, who may have long term broad knowledge of the industry, but lack the quantitative literacy to understand, for example, the internal models used by a bank to manage its capital adequacy within regulatory limits. The implication is that there is an imbalance in the knowledge of operational versus risk staff, and risk staff versus the Board members.

Expanding on this idea, there is growing evidence of problems of misunderstanding between accountants and traders in relation to the value of complex derivatives. The risk imbalances in the trader-accountant relationships are exacerbated when the products are illiquid and the valuation primarily comes from traders. These can be complex and hard to value. Valuation quotes for illiquid products may come from a single broker, making such quotes subject to manipulation given the existence of a good personal relationship between the trader and the broker. If the illiquid products are marked to model, the valuation is first determined by the traders before going through a price testing process by the product controllers. This valuation process creates a risk imbalance as the valuation is largely driven by the traders and in practice it is difficult for product controllers to challenge or override the traders' valuation of illiquid products.

Goldstein and Henry (2007) cite evidence from the financial crisis of traders (who designed or sold products) being responsible for the models used in their valuation, which were accepted by accountants who lacked the knowledge to effectively challenge the valuations. The risk imbalance comes from risks of errors in model, input and parameter specifications, where the expertise falls primarily with the traders. The product controllers typically run the models which have been pre-validated. Even if the theoretical knowledge gap can be mitigated by better training of accountants and auditors, the traders are still ahead of the curve by virtue of their closeness to the business environment. The traders can claim to know the business and to have the more relevant 'market' prices for product valuation in financial reporting. The traders also generate significant revenues for the banks and are duly bestowed significant power and status within the organization relative to the accounting, control and risk management staff. This power can be seen in the millions of dollars of loss limits that a single senior trader can have in the bank. The recent LIBOR rigging scandal is evidence of the disproportionate power that traders can exercise within banks, but such power, when misused, can have disastrous consequences for the institution.

In practice, a challenge process places the onus/burden on the product controllers to disprove the traders' valuation. This process assumes the traders' valuations are correct by default unless proven otherwise. Usually there is lack of evidence to override the traders' valuations when the markets are illiquid. In illiquid markets, the mark-to-market movements (in billions of dollars) are mainly decided by the traders. When the valuations become critical to the stock market perceptions of the firm's viability, senior management gets involved in the valuation process which creates further pressures on the valuations by the product controllers whose roles are relegated to "starting conversations". In the case of Lehman Brothers,

> "Jonathan … Head of the GREG Product Control Group, recalled an incident in the second quarter of 2008 that made him uncomfortable with the degree to which senior management was involved in the valuation process. Jonathan … proposed to

> Kenneth …, Head of U.S. Originations for GREG, that certain positions for which Kenneth … was responsible be written down. … Jonathan … recalled that Kenneth … replied that 'I can't take it right now.' It was Jonathan …'s impression that Kenneth … did not have the authority to take the writedown. Jonathan … raised the issue with the CFO … was uncomfortable that he was forced to go high up the chain to get approval to take the write-down, but approval was eventually given. Jonathan … told the Examiner that 'in the end, all I can do is price test – the front office owns the mark' and 'all I can do is start the conversation.'" (Jenner and Block, 2010)

The resilience of the valuation process appears to depend on the trading positions taken by the traders relative to the size of the controller team. The Lehman case illustrates how the risk imbalances between the traders and the product controllers got exacerbated during the credit crisis. A crisis is a time when traders can wield considerable power over the valuation process which affects financial reporting and take advantage of the risk imbalances caused by market illiquidity and mounting pressure over the financial numbers.

Information asymmetry also arises between traders and trader management. Willman et al. (2002) alluded to a potential control problem: namely, that managers place faith and trust on the integrity and competence of traders and give them extensive autonomy (one trader commenting: "I have a direct boss who is theoretically my boss, but he does not get involved in anything at all"). Despite the managers being largely former traders, they found it difficult to have full knowledge of all the trader positions. The traders draw power from the information asymmetry between themselves and the people controlling them, allowing them to exploit risk imbalances.

Risk imbalances due to knowledge gaps were also causes of risk management failures in major trader scandals involving banks such as Barings and Société Générale. In these cases, the traders had in-depth knowledge and experience of the middle and back office operational processes, in addition to their trading experience, and utilised that knowledge to their benefit. The trader in Société Générale used the amendment and cancellation function of the trading system to input one-sided trades and to generate fictitious profits. He also masked losses by inputting fictitious contracted rates in the trading system before its end-of-day batch run and reversing these trades before the start of the back office deal matching process. In Barings, the FX trader observed that slight errors in trading slips were booked against an error account in London with small positive and negative errors netting close to zero over time. The FX trader used this knowledge to hold large FX positions overnight and rolled them to larger FX positions when losses accumulated, at the same time showing large profits. In both cases, the traders' knowledge of the intricate operational processes created significant risk imbalances, enabling the traders to exceed their loss limits and to generate billions of dollars of losses.

Table 1 also denotes the limited risk literacy of the Board of Directors as a potential source of risk imbalance. This lack of specialised knowledge on the part of the Board echoes the imbalances in the control environment relating to poor leadership and lack of engagement on the part of Board members. This linking of information based imbalances with the control environment provides further evidence that the three sources of risk imbalance shown in Table 1 are interdependent. A weak control environment may incorporate imbalances that are aggravated within the risk architecture. Information and the power to exercise control is the glue that holds the risk management system together, and so when one party has an advantage over another in either of these respects, the result is imbalance across the entire system and a potential risk management disaster.

The evidence presented above indicates that risk imbalances play a very important role in determining the level of effectiveness of risk management systems and particularly ERM. More importantly, the multiple sources – both internal and external- of such imbalances suggest that the idealised blueprint of risk management may ultimately be unachievable. Complex amalgams of internal and external forces interact to limit the effectiveness of formal risk management systems and in the next section we use a single case study to illustrate how these imbalances can interact to cause serious control problems. We illustrate the argument with the case of Barclays bank, which appeared to survive the financial crisis well, but suddenly found multiple cracks in its risk management system.

Case Study

The 2009 Reported profits for Barclays plc exceeded analyst's expectations and were almost double those of 2008. Furthermore, the bank was one of the few in the UK that did not need a direct capital injection from the government to survive the financial crisis although it did benefit from the systemic support offered to the sector. Barclay's resilience in the face of a global crisis that brought a number of banks down, led many to take the view that their risk management system was robust and effective.

That view was, however, turned around by a series of events that hit the bank hard post 2010. In 2011 Barclays became the first UK bank to apologise to its customers for the scandal surrounding the mis-selling of personal protection insurance (PPI) and they set aside £3.2bn to compensate customers. In the light of larger than expected claims, Barclays were forced to increase the provision for compensation by a further £700 million in September 2012.

In June 2012 Barclays was fined £290m after some of its derivatives traders were found to have attempted to rig the London Interbank Offer Rate (LIBOR), a key figure that forms the basis for multiple interest rate based deals across the UK. Evidence suggests that misconduct was widespread, involving staff in New York, London and Tokyo as well as external traders. A report by the FSA (FSA,2012) suggests that between January 2005 and June 2009, Barclays derivatives traders made a total of 257 requests to fix Libor and Euribor rates.

In response to these, and other criticisms of its governance processes, Barclays commissioned the Salz Review into its business practices. The review was published in April 2013 and it highlighted the problems created within the bank by its rapid rise from a domestic retail bank into a global institution. The report noted a downward spiral in governance standards within Barclays, that was compounded by a heady mix of growing business complexity and a changing organisational culture that emphasised profit growth.

Using evidence from the Salz Review, Table 2 shows the presence of an accumulation of risk imbalances both within Barclays itself and also within its regulatory environment. The control environment within which the bank operated, was one of "light touch" regulation, but this approach enabled (if not) encouraged Barclays to focus on compliance with the letter rather than the spirit of the law. As a result, they engage in activities which were described as "pushing the envelope" in terms of their acceptability within the regulations. In such a situation it can be argued that it is compliance, rather than risks that are being managed and hence there is a major risk imbalance.

Similarly, the Basel reporting requirements encouraged the adoption of a silo based approach to risk management, which categorised risks under the headings of market, credit, liquidity and operational risks. Market commentators acknowledge that in the crisis Barclays managed their market, credit and funding risks well, but they failed to pay attention to operational and reputational risks. The PPI and LIBOR scandals reflect operational failures that have hit the bank's reputation very hard. In other words, managing in silos means that the eye can be taken off the ball in key areas. The theory of ERM is that oversight should be holistic in orientation, not silo based.

The architecture of risk management within Barclays also undermined its effectiveness, by granting limited status to the Chief Risk Officer and the wider function of risk management. Within a divisionalised business, the professionalization of the risk management function left operational staff unclear about their lines of responsibility, even though the three lines of defence model portrays them as the first line of defence. Furthermore, the lack of representation of the risk management function on the group's executive committee left them without a voice in strategic decision making. In other words, the second line of defence lacked any muscle.

Perhaps the most damning indictment from the Salz review relates, however, to the culture within Barclays, or what we term in our model the organisation's sharing of information and understanding of risk. Within the divisionalised structure some sections of the bank took an adversarial approach towards compliance. Key lines of responsibility within the risk management function were confused and the Board of Directors were limited in their levels of risk literacy. In other words there was no common understanding of the level of risk to be taken, the actual level of exposure nor the case for sanctions when risk limits were breached.

The fault lines, or imbalances in the risk management system within Barclays are detailed in terms of our model in Table 2. Given the overall level of these imbalances, it is perhaps not surprising then that Barclays succumbed to a series of risk management failures. These failures can be explained by the application of the Swiss Cheese model of risk management, as explained below.

The Swiss cheese model

Reason's (2000) Swiss cheese model (see Figure 1) portrays risk management as a series of slices of cheese that act as defences against the impact of "holes" or ineffective controls that may arise because of either active failures in control systems e.g. IT breakdown or what he describes as latent conditions that can cause holes in the defence slices. These latter are caused by inherent weaknesses in the defences that increase their susceptibility to failure, such as an organisational culture that does not see risk management as important. The Swiss cheese analogy is critical because Swiss cheese is characterised by its many holes. If the holes represent weaknesses in the defence system, but those in adjacent slices do not line up, then the risk management defence system is not penetrated to a degree where major losses are incurred. If, however, the holes in successive slices are in alignment, then risks are crystallised and the organisation incurs losses, or, in extremis, major risk management failure.

The risk imbalances outlined in Section 3 may occur within a company's control environment, risk architecture or the overall information and understanding of risk. If the imbalances are

redefined as equivalent to holes in Reason's model, then one-off holes may not matter. A company can manage isolated failures in its control system. If, however, many different holes occur together and are aligned, then the overall system comes under threat of failure, even if the individual lines of defence are in place. We would argue that Barclays plc provides an example of how seemingly good defence systems can be undermined by risk imbalances. The powerful latent forces of a divisionalised business model, combined with a lack of common purpose about risk management across the bank combined to produce the ingredients for failure. There is an element of randomness in the fact that the holes may/may not align, but if they do then problems abound.

The central lesson of the Swiss cheese model is that defence structures alone are not sufficient. How they interact is also of critical importance, but this is a mtter of human relations, and issues of relative knowledge and power.

Conclusion

The literature on ERM has, to date, been largely silent on the question of levels of knowledge and power within risk management systems. The focus has instead been on the levels of take-up of ERM and consideration of alternative frameworks of implementation within individual organizations. This focus on the analysis of frameworks and committee systems can be criticised for its emphasis on bureaucracy at the expense of the human dimension that inevitably impacts upon the effectiveness of risk management in practice.

The motivation for this paper was the lack of critical empirical research looking at the social and political context of ERM and the resulting problems that posed for its implementation. We are searching for explanations for the mismatch between ERM in theory and in practice. The framework of risk imbalances that we have outlined indicates that ERM is much more than a set of structures and reporting lines because it involves numerous different risk actors, many of whom have varying perspectives which may potentially be in conflict with one another. Consequently, ERM implementation is hampered by failures of collaboration both within and outside the organization.

A failure to consider the human dimension of risk management is particularly prevalent within the financial services sector where risk management has come to be expressed in terms of numbers and mathematical models. The emphasis on quantitative modelling has led to a belief that once risks are known – i.e. quantified, they can be managed. Even difficult risks, such as subprime mortgages can be managed if we can quantify the likelihood of default, but ultimately organizations are still left with the uncertain elements, or risks that cannot be managed. These are the things that firms could get blamed for if things go wrong, and so risk management has evolved into a discipline that seeks to convert things into manageable categories that provide managers with the excuse that "things went crazy", or "the scenarios were too extreme to be imagined". Such excuses suggest that the field of vision of risk managers is strictly limited as they try to manage risk rather than engage with it. What is more, the Swiss cheese model suggests that risk management systems alone are not enough.

In other words current risk management practice is seeking to create a false sense of certainty, whereas what is perhaps needed is more creativity in risk management. Extending the field of vision to include the possibility of acknowledging and addressing risk imbalances turns ERM into a truly holistic process that has human as well as mechanistic components.

The financial crisis has led to multiple reports and reviews of what went wrong, and the list of possible solutions gets longer by the day. The Institute of International Finance (2008) recommends that board members should be educated in risk management and measurement so that they can better understand their company's performance and exposure against the desired risk appetite. Others, such as the Committee of European Banking Supervisors, argue that there is a need for greater regulatory guidance on issues of risk culture, risk appetite and risk tolerance (CEBS, 2010). More fundamentally, it is suggested that there is a need for a "crucial shift in regulatory philosophy" which looks at systemic risks and the sustainability of business models rather than assuming that all risk can be identified and managed at the level of the individual firm (p.94, Turner, 2009). Sadly, however, all of these proposed solutions are incomplete as they emphasise the mechanics and not the people.

The 18 high profile risk management crises analysed in the "Roads to Ruin" report were classified as being caused by poor board leadership, a limited field of vision in identifying risks, poor communication, inappropriate incentives and a glass ceiling that prevents risk managers from being heard at the highest level in an organisation. These are all risks which arise out of the imbalances illustrated in this paper and they will not be resolved simply by further regulation.

.

Table 1: Origins and forms of Risk Imbalances

	Form of the Risk Imbalance	
Source of the Risk Imbalance	**Internal**	**External**
Control environment	• "Tone at the top" • Remuneration systems	• Regulation leads to better governance and risk management • "Light touch" regulation of large financial institutions
Risk architecture	• Presence and status of CRO • Professionalisation of risk management • Silo based thinking	• Generic(COSO) v sector specific systems (Basel II) • Compliance versus enterprise risk mindsets • Greater regulation encourages regulatory arbitrage . • Role and power of credit rating agencies

Information and/or understanding about risk	• Traders versus internal controllers e.g. accountant or internal auditor • Board of Directors' knowledge and risk literacy	• Excessive complexity of regulation • Sharing (or lack of) information between auditors the organisation and regulators • Information asymmetry between an organization, stakeholders and regulators

Table 2: Chief Risk Officer Status in Major Global Banks

BANK	CHIEF RISK OFFICER	MAIN BOARD MEMBER	REPORTS TO:	BOARD RISK COMMITTEE
Barclays	Y	N	Group Finance Director	Y
Royal Bank of Scotland	Y (Deputy –see column 3)	N	Head of Group Restructuring & Risk	Y
HSBC	Y	Y	Unclear	Y
JP Morgan Chase	Y	N	CEO	Y
Bank of America	Y	N	CEO	Y
Deutsche Bank	Y	N (Management Board but not Supervisory Board member)	Chair of Supervisory Board	Y

Table 2: Cumulative Risk Imbalances within Barclays Bank

	Form of the Risk Imbalance	
Source of the Risk Imbalance	**Internal**	**External**
Control environment	• **"Tone at the top"** Unwillingness to hear "bad news"; employees should solve problems. Lack of emphasis on staff training and development Did not give sufficient attention to leadership & governance. • **Remuneration systems** Emphasised and rewarded revenue generation. Focus on current year bonuses not sustainable profit.	• **"Light touch" regulation** Facilitated a focus on the letter of the law rather than the spirit. Pushing the envelope to the limits e.g tax structuring schemes.
Risk architecture	• **Presence and status of CRO** 2004 CRO left Executive Committee so 2006-9 (crisis period) no group risk representative on Executive Committee. CRO not involved in remuneration committee discussions. Head of compliance reports to • Professionalisation of risk management	• **Compliance versus enterprise risk mindsets** Risk structures in bank reflect the Basel risk reporting ystems • **Greater regulation encourages regulatory arbitrage** "Strained" relationship with regulators. e.g. engagement in regulatory arbitrage over capital requirements

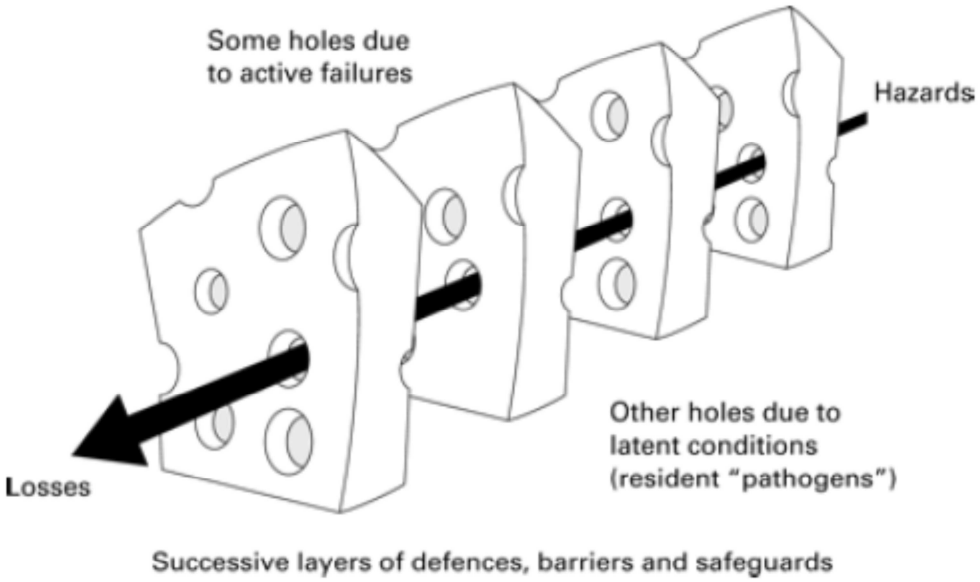
	Lack of clarity of lines of responsibility for risk amongst operational managers • **Silo based thinking** Inconsistencies in risk appetite across the group. Credit, market and funding risks were well managed but operational, conduct and reputational risk less valued.	
Information and/or understanding about risk	• Decentralised business model made "three lines of defence" model difficult to implement • Adversarial attitude within the investment bank towards the compliance function • LIBOR scandal indicated power of traders relative to risk officers within the bank and a culture tolerant of such behaviour • Provisions needed to cover fines and penalties for PPI mis-selling • Division of responsibility between Group Head of Compliance and Regulatory Relations serves to confuse lines of accountability.	• Excessive complexity of regulation

	• In some business units front office staff unsure of their role in relation to risk management and control • Lack of common purpose and shared values within the bank. • Board of Directors' knowledge and risk literacy	

In June 2012, Alistair Darling, his predecessor as Chancellor, said in relation to the involvement of Barclays' traders in the LIBOR scandal: "Quite clearly, there was a culture here that tolerated – if it didn't encourage – this sort of behaviour.

Daily Telegraph, "Barclays culture 'encouraged' abuse, says Alistair Darling", 28 June 2012.

Figure 1 Swiss Cheese Model



References

Airmic/Cass (2011), *Roads to Ruin: A study of major risk events. A report by Cass Business School on behalf of Airmic.* London, UK.

Airmic, ALARM, and IRM (2010), A *structured approach to Enterprise Risk Management and the requirements of ISO 31000*, (http://www.airmic.com/research/guides).

Arena, M., Arnaboldi, M. and Azzone, G. (2010), "The organizational dynamics of Enterprise Risk Management." *Accounting, Organizations and Society*, Vol.35 (7), pp.659-675

Ashby, S., Sharma, P. and McDonnell,W. (2003), *Lessons about Risk: Analysing the Causal Chain of Insurance Company Failure.* Prudential Standards Division, Financial Services Authority, London.

Asher, A. and Heaser, C. (2008), *AIG Collapse - Putting the Pieces Together. What can we Learn?*, (http://www.deloitte.com/assets/Dcom-Australia/Local%20Assets/Documents/Deloitte_AIG_credit_crunch.pdf).

Basel Committee (2010), *Principles for enhancing corporate governance*, Basel Committee on Banking Supervision, Basel, Switzerland.

Beasley, M. S., Pagach, D. and Warr, R. (2008), *The Information Conveyed in Hiring Announcements of Senior Executives Overseeing Enterprise-Wide Risk Management Processes.* Journal of Accounting, Auditing, and Finance, Vol.23 (3), pp. 311-332.

Beck, U. (1992), *Risk Society — Towards a New Modernity*. London: Sage.

Boyls, G. (2010), *The Financial Crisis and Enterprise Risk Management - AMX International Incorporated*, (http://www.amxi.com/images/The_Financial_Crisis_and_Enterprise_Risk_Management.pdf).

Buffett, W. E. (2001), *Letter to the Shareholders of Berkshire Hathaway, November 9, 2001*. Omaha.

Caplain, B. (2008), Risk Management: Why It Failed, How to Fix It. Internal Auditor. Downloaded from http://www.theiia.org/intAuditor/feature-articles/2008/december/risk-management-why-it-failed-how-to-fix-it/ on 14/01/13.

Chesney, M., Stromberg, J. and Wagner, A. F. (2010), *Risk-taking incentives, governance, and losses in the financial crisis,* Swiss Finance Institute Research Paper. Available at: SSRN: http://ssrn.com/abstract=1595343.

Committee of European Banking Supervisors (2010), *High level principles for risk Management.London,UK.*

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2004), *Enterprise Risk Management – Integrated Framework. Executive Summary.* AICPA,New York, NY.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2011), *Internal Control – Integrated Framework.* AICPA,New York, NY.

Culp, C.L. (2002), "The Revolution in Corporate Risk Management: A decade of innovations in process and products." *Journal of Applied Corporate Finance*, Vol.14 (4), pp.18-26.

Deloitte (2011), *Global Risk Management Survey*, 7th Edition. Deloitte Global Services Ltd.

Dewing, I.P. and Russell, P.O. (2012), "Auditors as regulatory actors: the role of auditors in banking regulation in Switzerland" *European Accounting Review*,Vol.21 Issue 1, pp1- 28.

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

Erkens, D., Hung, M. and Matos, P. (2009), *Corporate governance in the 2007–2008 financial crisis:evidence from financial institutions worldwide*, ECGI Working Paper.

Available at: SSRN:http://ssrn.com/abstract=1397685.
FRC (2008), Financial Reporting Council. *The Combined Code on Corporate Governance.* June. London.
FRC (2011), Financial Reporting Council 2011. *The impact and implementation of the UK corporate governance and stewardship codes.* December. London.
FSA (2008), *The supervision of Northern Rock:a lessons learned review.* Financial Services Authority, London.
FSA (2009), *The Turner Review. A regulatory Response to the Global Banking Crisis.* Financial Services Authority, London.
FSA (2011), *The failure of the Royal Bank of Scotland*, Financial Services Authority, London.
G20 (2008), *Declaration of the Summit on Financial Markets and the World Economy.* Office of the White House press secretary, November 15, Washington.
Graybow, M. (2008), "Credit Rating Agencies Fending Off Lawsuits from Subprime Meltdown", Insurance Journal.com http://www.insurancejournal.com/news/national/2008/07/14/91841.htm (accessed 15th September 2008)
Guerrera,F. and Thai-Larsen,P. (2008), *Gone by the Board: why the directors of big banks failed to spot credit risks.* Financial Times,26 June.
Gupta, P. (2006), "Internal Control. COSO 1992 Control Framework and Management Reporting on Internal Control: survey and Analysis of Implementation Practices". IMA,Montvale, NJ.
Hoyt,R.,E., and Liebenberg, A.,P. (2011), "The value of Enterprise Risk Management", *The Journal of Risk and Insurance*, Vol.78 (4), pp.795-822.
Humphrey, C., Loft, A. and Woods, M. (2009), "The global audit profession and the international financial architecture: understanding regulatory relationships at a time of financial crisis", *Accounting, Organizations and Society*, 34(6/7), pp. 810-825.
IFAC/CIMA (2002), *Managing risk to enhance shareholder value.* International Federation of Accountants, New York.
Institute of International Finance (2012), "IIF Response to the Global Financial Crisis 2007-12.Washington.
ISO (2009), *'ISO 3100: Risk management-Principles and guidelines'*. International Organization for Standardization, Geneva, Switzerland.
Jenner & Block. (2010), *Lehman Brothers Holdings Inc. Chapter 11 Examiner's Report*, Jenner & Block LLP, New York, US. (http://lehmanreport.jenner.com)
Kajuter, P., Linsley, P., and Woods, M. (2007), Risk Management, Internal Control and Corporate Governance: International Perspectives in Woods, M.,Linsley,P., & Kajuter, P. (Eds.), *International Risk Management: Systems, internal control and corporate governance*, Elsevier.
KPMG (2011), *Risk Management: A driver of enterprise value in the emerging environment*, KPMG International.
Ladipo, D., Nestor, S. and Risser, D. (2008), *Board Profile, Structure and Practice in Large European Banks – A Comparative Corporate Governance Study*. Research Report by Nestor Advisors,London. Available at: http://www.nestoradvisors.co.uk.
Livne, G. and Markarian, G. (2010), *Investment horizon, risk, and compensation in the banking industry*, Cass Business School Working Paper
Magnan, M., and Markarian, M. (2011), Accounting, governance and the crisis: Is risk the missing link? *European Accounting Review*, 20(2), pp.215-23.
Marks, N. (2011), *COSO ERM- A good framework? Institute of Internal Audit.* Downloaded from http://www.theiia.org/blogs/marks/index.cfm/post/COSO%20ERM%20-%20A%20Good%20Framework

Martin, D., and Power, M. (2007), *The end of enterprise risk management*. Aei-Brookings Joint Center for Regulatory Studies, August (07-22).
Mikes, A. (2009), "Risk management and calculative cultures", *Management Accounting Research*, 20(1), pp. 18-40.
OECD (2004), *Principles of Corporate Governance.* Paris, France.
OECD (2009), *The Corporate Governance Lessons from the Financial Crisis.* Paris, France.
Power, M. (2005), "Organizational responses to risk: the rise of the Chief Risk Officer", in Hutter, B. and Power, M. (Eds.), *Organizational Encounters with Risk*, Cambridge University Press, Cambridge, UK, pp. 132-148.
Power, M. (2007), *Organized Uncertainty, Designing a World of Risk Management*, Oxford University Press, Oxford, UK.
Power, M. (2009), "The risk management of nothing", *Accounting, Organizations and Society*, 34(6/7), pp. 849–855.
PwC (2007), *Creating value: Effective risk management in financial services.* PricewaterhouseCoopers Global Financial Services.
PwC (2012), *Black swans turn grey – The transformation of risk*, January, PwC UK.
Reason, J. (2000) Human Error: Models and Management, *British Medical Journal*, 320:768-70.
Rebonato, R. (2007), *Plight of the Fortune Tellers. Why we need to manage financial risk differently.* Princeton University Press. Oxford, UK.
Roberts, J. (2009), "Faith in the numbers", *Ephemera*, 9, pp. 335-343.
Saul, J.R. (1993), *Voltaire's Bastards: The Dictatorship of Reason in the West.* Vintage Books, USA.
Senior Supervisors Group (2009), *Risk Management Lessons from the Global Banking Crisis of 2008*, October.
Smithson, C. and Simkins, B. J. (2005), Does Risk Management Add Value? A Survey of the Evidence, Journal of Applied Corporate Finance, 17: 8-17.
Taleb, N.M. (2007), *The Black Swan: The Impact of the Highly Improbable.* Penguin Books, London,UK.
Tett, G. (2009), *Fool's Gold*, Little Brown Book Group, London, UK.
Walker Review (2009), *A review of corporate governance in UK banks and other financial industry entities*. November, London.
Wahlstrom, G. (2009), Risk management versus operational action: Basel II in a Swedish context. *Management Accounting Research*, Vol. 20, pp. 53–68.
Wacek, M.G. (2011), *Derivatives, AIG and the Future of Enterprise Risk Management*, (http://www.scribd.com/doc/38923886/Derivatives-AIG-and-the-Future-of-Enterprise-Risk-Management).
Wheelhouse Advisors. (2009), *A Recipe for Disaster*, (http://wheelhouseadvisors.wordpress.com/2009/03/30/a-recipe-for-disaster/).
Whitehead, Alfred North (1925), *Science and the Modern World*, Cambridge: Cambridge University Press.
Woods, M. (2009), "A contingency theory perspective on the risk management control system within Birmingham City Council", *Management Accounting Research*, 20(1), pp. 69-81.
Woods, M. (2011), *Risk Management in Organizations: An integrated case study approach.* Routledge, Abingdon,Oxon.
Young, J. (2001), Risk(ing) metaphors. Critical Perspectives in Accounting, Vol. 12, pp. 607–625.