UNIVERSITY OF GOTHENBURG
SCHOOL OF BUSINESS, ECONOMICS AND LAW

Operational Risk Management

A Case Study at a Global Financial Institution

Robert Rempfler

Graduate School
Master of Science in Management
Master Degree Project No. 2011:130
Supervisor: Gudrun Baldvinsdottir

Abstract

The financial crisis has led to reconsider how financial institutions manage their risks. Despite for the recognized importance of operational risk, credit and market risk have attracted most of the attention so far. This paper argues that managers at business unit levels are responsible for managing operational risk but have little guidance. Regulators direct their efforts at the corporate level and the academia focuses on quantitative approaches. As a result of the lack of guidance, operational risk management emerges as a pragmatic and reactive process. Additionally, although regulators stress the importance of independent control, the paper recognizes business embeddedness as a critical feature for the successful management of operational risk at the business unit level. Last but not least, the results show that operational risk management is often associated to the issue of bureaucratization.

Acknowledgments

First of all I would like to thank the risk manager of the business unit for for the tireless support and the interesting discussion on the topic of risk management and operational risk. Also, I would like to show my gratitude to my supervisor, Associate Professor Gudrun Baldvinsdottir for her dedication and commitment. Moreover, this research would not have been possible without the efforts and thoughts of all the interviewed persons; thank you.

Abbreviations

AMA – Advanced Measurement Approach (Basel II; BCBS, 2006)

BBA – British Bankers Association

BoD – Board of Directors

BIS – Bank of International Settlement

BCBS – Basel Committee on Banking Supervision

CRO – Chief Risk Officer

OC – Operational Committee

GEB – Group Executive Board

IA – Investment Advisory

IPS – Investment Products and Services

MC – Management Committee

ORAP – Operational Risk Assessment Process

ORC – Operational Risk Control

ORF – Operational Risk Framework

ORI – Operational Risk Inventory

ORT – Operational Risk Taxonomy

QRM – Quality and Risk management

TPR – Transaction Processing Risk

Introduction

The financial crisis that erupted in 2008 had severe consequences for financial corporations. The magnitude of the events has stressed the inadequateness of the existing risk frameworks and has led to reconsider how financial institutions manage their risks (Bessis, 2010). The crisis was triggered by the downturn in the US housing market. However, other elements have to be included in order to get a better picture of what happened. Financial engineering, securitization, leverage, risk modelling practices, and contagion dynamics (Cline, 2010) led the crisis, initially limited to the US housing market, to a systemic "credit crunch" that jeopardized the whole financial system (Bessis, 2010). The initial source of the crisis can be identified in both market and credit risk, i.e. adverse price movement of the US housing prices and the default of mortgages that followed. However, it is argued that the reasons for which the US sub-prime turmoil ended up collapsing the overall financial system are also to be found into business practices, i.e. operational risk (Bessis, 2010; Cline 2010). Just to mention a few examples: failure to properly identify exposure to market/credit risk; losses related to reputational risk; risk management processes; conflict of interest, product risks and client suitability, etc.

Guided by different motivations, practitioners, regulators and academics have devoted great resources in understanding what happened and how to prevent it from happening again. Consistently with the industry bias[1], credit and market risk management practices attracted most of the attention (Bessis, 2010).

This is alarming and at the same time confusing because by now the importance of operational risk has been recognized. Significant corporate operational losses[2]; advancements in information technology and telecommunication (Hussain, 2000; Buchelt and Unteregger, 2004), deregulation on volumes and operations (Chernobai et Al., 2007); globalization and fundamental changes in the financial markets (Chernobai et Al., 2007); financial product complexity and decentralized control (Halperin, 2001) have raised the profile of operational risk. As argued by Buchelt and Unteregger (2004) operational risk is not a second-priority risk, it is much greater than market risk. Moreover, quantitative studies (Cummins et Al., 2006 ; Wei, 2006 ; Wei, 2007) also highlighted the

[1] In the past, banks have been considered to face the biggest risks in credit and market exposure (Chernobai et Al., 2007)

[2] To mention a few: Orange County, 1994 (US); Barings Bank, 1995 (UK); Daiwa Bank, 1995 (US); Allied Irish Banks; 2002 (IRL) Marshall (2001), states that the aggregate losses due to operational risk during the period 1980-2000 in the financial industry account for USD 200 Billions. With single corporations facing losses larger than USD 500 Millions in 50 instances and over USD 1 Billion in approximately 30 cases. For additional information about the scandals related to weak operational risk management please refer to Hussain (2000); Marshall (2001); Chernobai et Al. (2007)

importance of operational risk by demonstrating that a financial institution facing an operational loss will suffer a market value decline that is greater than the loss per se.

Finally, the emergence of operational risk as a first-priority risk was institutionalized in 2006 with its inclusion in the Basel II Framework[3] (BCBS, 2006). However, because of their ultimate goal of achieving financial stability and avoiding systemic failure (BIS, 2010), regulators have emphasized the capital requirements of banks (partially as a function of operational risk) and therefore encouraged the measuring rather than the managing of operational risk (Rebonato, 2007).

After the issuance of Basel II (BCBS, 2006) with particular emphasis on AMA (Advanced Measurement Approach) the academia and risk professionals (GARP, CFA, etc.) have developed a notable amount of literature discussing quantitative approaches (risk modelling) to establish the capital requirement of financial corporations (e.g. Cummins et Al., 2006; Rosenberg and Schuermann, 2006). However, besides for the shortcomings of applying quantitative methods to operational risk[4], attention should be devoted to how operational risk is managed rather than measured. Shareholders demand an effective, and possibly efficient operational risk framework, not developed measurement practices.

Recently, with the issuing of the Sound Practices for the Management and Supervision of Operational Risk (BCBS, 2011) regulators have provided an improved framework for managing operational risk as well as signalling the interest in managing, rather than measuring operational risk. Despite for the soundness of the eleven principles outlined in the framework, because operational risk is diverse and specific to each corporation (Moosa, 2007), the document has a "macro-approach" that sets out general guidelines that are easy to “check”. On top of that, while regulators address the highest authorities of the bank, it is claimed that middle and lower management is responsible for managing operational risk, not the CEO nor the BoD (Buchelt and Unteregger, 2004 and Rao and Dev, 2006).

Summing up, risk management practices are in the spotlight and the importance of operational risk has been recognized. Regulators deliver general principles to the highest authorities of financial

---

[3] It is interesting to not that credit risk was regulated in 1988 and market risk in 1996. Credit risk was regulated through the introduction of a capital requirement known as “Cooke Ratio”. The ratio is calculated as the amount of capital a bank has to have in relation to its total risk-adjusted assets while market risk was regulated through the introduction of VaR (Value at Risk) requirements

[4] Among others, the key issues of applying quantitative models to operational risk relate to its fat tail distribution (Chernobai et Al., 2006) and the lack of robust data (Muzzi, 2003) which also includes the difficulties associated to quantifying non financial events, e.g. business disruption. Additionally Marshall (2001) argues that modeling human errors is particularly challenging

institutions even though middle and lower management is expected to manage operational risk. Therefore, in the light of what is stated so far, middle and lower management has responsibility but at the same time discretion over how to manage operational risk.

Purpose, research question and structure of the paper

Because the concept of operational risk is nebulous (Power, 2004), it is important to start with a conceptual definition. To clarify this, the first part of the paper looks at how global financial organizations understand operational risk.

Research Question 1: How do global financial organizations understand operational risk?

Once the reader is familiar with the conceptual aspects of operational risk the paper presents how operational risk is managed at the corporate level. Thereafter, since middle and lower management is responsible for managing operational risk the paper looks into theories about operational risk management. This leads to the second part of the paper where operational risk management is explored at business unit level.

Research Question 2: How is operational risk managed at a business unit level?

The first part of the paper will contribute to the existing academic literature by shedding light on the conceptual aspects of operational risk. The second part of the paper will provide the academic literature with an alternative understanding of how operational risk is managed. The evidence provided in the study clarifies the complexity associated with regulating and framing operational risk. Finally, by taking a new standpoint on the topic of operational risk management, the paper identifies and encourages new research openings.

Frame of Reference

Risk and operational risk

In the financial industry the definition of risk depends on the context and the purpose for which one wishes to formulate the concept of risk (Chernobai et Al., 2007). When applied to operational risk management practices, risk is commonly understood as the potential of sustaining a loss (Bessis, 2010), i.e. risk is associated to a negative outcome only.

According to Chernobai et Al. (2007), corporations active in the financial industry face four main types of risks:

1. *Credit risk* – the risk that a counterparty will not be able to fulfil its financial commitment
2. *Market risk* – the risk of an adverse price movement in the market

3. *Operational risk* – the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events[5] (BCBS, 2001)
4. *Other risks* – a residual risk group that captures risks such as strategic risk, political risk, etc.

Banks are considered to face the biggest risks in the first two risk groups (Chernobai, et Al., 2007; Bessis 2010). However, the view of operational risk as a less influent risk has been overruled by several researchers (e.g. Halperin, 2001; Blunden, 2003; Buchelt and Unteregger, 2004; Cummins et Al., 2006; Wei, 2006) and its emergence as a primary risk was officially recognized in 2006 with its inclusion in the Basel II Framework (BCBS, 2006).

As argued by Rao and Dev (2006), in the past everything other than credit or market risk was by default operational risk. Today, the definition of operational risk provided by the BCBS is much more sophisticated, i.e. "The risk of loss resulting from inadequate or failed internal processes, people or systems, or from external events" BCBS (2001). The definition is widely accepted, both, by the academia and practitioners. However, despite the general acceptance of the definition provided by the BCBS, most academic authors on operational risk still devote the first pages of their work to discussing its definition (e.g. Chernobai et Al., 2006; Bessis, 2010). This suggests that while its definition is accepted, its usage still needs to be justified.

Throughout the literature, five important traits of operational risk were identified. First, operational risk is diverse and multidimensional (Hoffman, 1998; Marshall, 2001; Milligan, 2004). On the same line, Buchelt and Unteregger (2004) describe it as a highly varied and interrelated risk that can stem from potentially infinite origins. Second, operational risk lacks a financial indicator and robust data. De Koker (2006) argues that while the logics of risk-return can be applied to credit and market risk, this is harder for operational risk as there is no closely relatable financial indicator. Also, a quantitative approach to operational risk is further complicated by the lack of robust data (Muzzy, 2003) and by the difficulty of modeling human behavior (Marshall, 2001). Third, operational risk is characterized by a heavy-tailed distribution (Moosa, 2007; Wei, 2007). Further evidence of this trait comes from the statement of Chernobai et Al. (2006) "operational loss […] is characterized by high kurtosis, severe right-skewedness, and a very heavy right tailed distribution". Fourth, operational risk is considered a cultural issue. As argued by Buchelt and Unteregger (2004), because of its diversity and business embeddedness, the handling of operational risk cannot be retained by the highest management. Therefore, operational risk management is described as a corporate activity

[5] Given the definition of the BCBS (2001), the concept of operational risk is very broad. It ranges from internal risks: IT failures, Transactional losses, Employee fraud or theft, Legal litigation, Product flaws, etc. to external risks: Natural disaster, Terrorism, etc.

rather than a managerial task, i.e. all employees and functions are involved with operational risk and thus it can be labelled as a "cultural risk" (Rao and Dev, 2006). Fifth, operational risk is considered to be more endogenous than credit and market risk (Moosa, 2007). By simply looking at the definition of operational risk, it is clear that its cause is more likely to be internal than external. The interesting aspect of viewing operational risk as an endogenous risk is that it rests within the control of the organization (Kaiser and Kohne, 2006).

Additionally, three important debated features of operational risk where identified: First, is operational risk one-sided[6]? Herring (2002) argues that operational risk can be defined as a "downside risk" because it is difficult to imagine a scenario in which operational risk leads to an unexpected profit. Lewis and Lantsman (2005) support this argument by arguing that operational risk is one-sided because only one-side probability of loss or no-loss exists. Following the same rationale, Crouchy et Al. (2004) stress that "by assuming more operational risk, a bank does not expect to yield more on average". From this perspective then, it is safe to conclude that a bank does not actively seek exposure to operational as the underlying assumption is that there is no reward from bearing operational risk (Ibid). On the other hand, according to Moosa (2007), banks do not expose themselves to operational risk because it is fun but because they can monetize such activities. Therefore the proposition that there is no reward from bearing operational risk is rejected. Moreover, the author argues that operational risk does not lead to a loss or no-loss situation because corporations "deliberately take on risk for the sake of potential reward, and in this sense [operational] risk cannot be one-sided" (Ibid), i.e. the positive side of the distribution curve is represented by the profits that materialize in the case of no operational risk loss.

Both sides have very strong arguments; it is suggested that the conflicting positions are the result of different starting assumptions. Whereas most of the authors consider operational risk as a by-product of financial corporations taking on credit and market risk (traditional view; e.g. Crouchy et Al., 2004), Moosa (2007) also includes those activities of the bank that are exclusively made up of operational risk (e.g. asset management, custodial service, etc.). On top of that, while Moosa (2007) directly implies business expansions to operational risk increases, this is not given in other authors' reasoning[7]. The viewing of operational risk as one sided is comfortable because, profits are hard to

[6] The term "one-sided" refers to the shape of the probability distribution curve of operational risk

[7] For example, an increase of operational risk might be related to inefficiencies in the management of operational risk; e.g. the usage of a new IT system might increase operational risk and is not necessarily followed by an increase of revenues or reduced costs. In his arguments, Moosa (2007) indirectly implies that corporations are efficient and that every time that operational risk is increased so will the revenues

impute to operational risk and also because such perspective emphasizes the need to increase efficiency. However, from a theoretical perspective, the view of operational risk as one-sided is faulty as it fails to see the "revenue side" of the distribution curve.

Second, is operational risk idiosyncratic? Lewis and Lantsman (2005) stress that operational risk is idiosyncratic because its manifestation is uncorrelated with market forces. Danielsson et Al. (2001), in their critique to Basel II state that operational risk is idiosyncratic because immune to contagion. On the other hand, there are four main reasons for which viewing operational risk as idiosyncratic can be considered wrong: 1) According to Moosa (2007) viewing operational risk as idiosyncratic is quite strange because it implies that if a bank incurs into losses from a loan default or market adverse movement, its ability of meeting its financial obligations will be affected, whereas the same is not true for operational losses. For example, if a bank faced a massive loss as a consequence of an adverse market movement on proprietary trading positions, the bank will have problems to pay back its debts to other financial institutions. However, a loss with the same magnitude would have no consequences for other financial organizations if it stemmed from operational risk[8]. This, is not consistent with what observed during the failures of Barings Bank (1995) and Long-Term Capital Management (1998/2000), where the overall system was affected (Bessis, 2010). 2) Given the objective of regulators, the simple fact that Basel II regulates operational risk is an indication that operational risk can have systemic consequences. 3) Bali and Allen (2004) make the general proposition that operational loss events incorporate cyclical components that are correlated with systematic risk factors such as macroeconomic fluctuations (implying that operational risk is not idiosyncratic). 4) Operational risk cannot be idiosyncratic simply because of the presence of groupthink (Moosa, 2007a). In the light of what stated above, the debate on the idiosyncratic feature of operational risk can be concluded in favor of its opponents. Not only viewing operational risk as idiosyncratic is misleading, it is also dangerous for the well functioning of the financial system.

Third, is operational risk indistinguishable from market and credit risk? The recent financial crisis highlighted that there is a strong interrelation between credit, market, and operational risk (Bessis, 2010; Cline, 2010). Also, as argued by Buchelt and Unteregger (2004), operational risk can materialize directly or indirectly through credit or market risk. However, according to Rebonato (2007) and Kaiser and Kohne (2006) the proposition that operational risk cannot be distinguished from credit and market risk can be rejected because by applying a cause-driven risk categorization the issue is solved. Despite for the benefits of a cause-based risk categorization, regulators have

[8] Financial corporations are strongly connected into a network of mutual financial obligations

decided to enforce an event driven risk categorization[9] (BCBS, 2006) as it allows to standardize risk exposures across the industry. Thus, the problematic of confusing operational risk with credit and market risk is likely to remain in the future.

Operational risk management

Operational risk management is typically understood as part of the broader concept of risk management (e.g. Allen et Al., 2004; De Koker, 2006; Chernobai et Al., 2007). However, operational risk, as opposed to market and credit risk, cannot be managed through quantitative approaches only. According to Marshall (2001), because operational risk is very diverse, its management implies several activities and disciplines that are not directly aimed at dealing with operational risk. For example, projects that aim at improving the quality of internal processes (e.g. TQM – Total Quality Management) can also be considered as operational risk mitigation actions. This implies that several aspects and departments of the corporation, through their daily activities are actually involved in the operational risk management (e.g. Insurance, Operations management, Audit, Compliance, Legal, Quality assurance, etc.). Therefore, in order to encompass the multidimensionality of operational risk, its management has to be approached in the most general way possible (Marshall, 2001).

Frameworks

The consulting industry, the academia, and practitioners have developed a limited set of operational risk frameworks that all look alike. The frameworks are not specific to financial corporations as operational risk is borne by all firms, regardless of the industry. In line with Marshall (2001), the few frameworks encountered maintain a very broad stance and never enter fine-grained aspects of operational risk. This happens for two reasons; first, the diversity of operational risk makes it hard to develop a fine tuned framework that remains encompassing. Second, because operational risk is specific to each organization, there is little use for a detailed framework as its usage is limited to the context it was developed for.

[9] Annex 9 of the Basel II framework – Detailed Loss Event Type Classification. Is an exhaustive list of all the possible operational risk events that can potentially arise. The list is based on 3 different levels of risk specification. At the first level the following groups of risk-events are identified: 1. Internal Fraud 2. External Fraud 3. Employment Practices and Workplace Safety 4. Clients, Products and Business Practices 5. Damage to Physical Assets 6. Business Disruption and System Failures 7. Execution, Delivery and Process Management

After an analysis of the different models offered (e.g. Marshall, 2001), it can be concluded that operational risk frameworks mainly revolve around four standard elements:

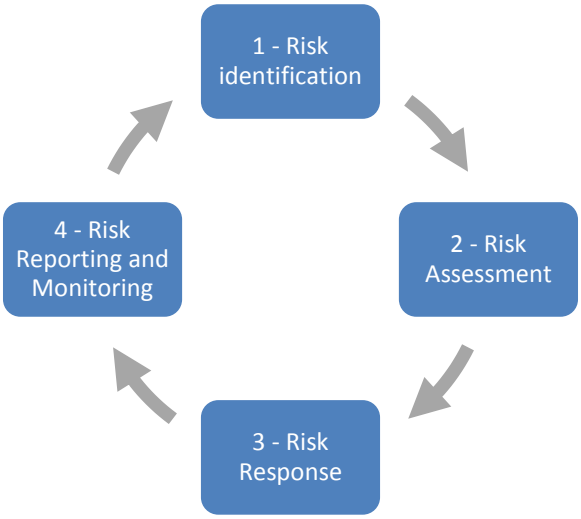

Figure 1: Standard Operational Risk Framework

1) Identification: through a data collection process risks are identified and classified (Marshall, 2001). The identification of operational risk is typically an employee's task while its classification is carried out by the risk manager. Among others, banks use the following risk identification sources: metrics; financial events; near misses; external events; audit reports; etc.

2) Assessment: the risk is assessed on the basis of its magnitude and frequency. The process is tedious and typically based on a quantitative approach[10] (Allen et Al., 2004).

3) Response: The risk assessment is compared with the risk appetite of the bank and the risk mitigation options are explored from a cost-benefit perspective. As result the corporation will decide if the risk is to be avoided, reduced, transferred or retained[11]. During this step managers are confronted with a strong conflict of interest: efficiency vs. control (Marshall, 2001).

4) Reporting and monitoring: risk information is disclosed to risk internal and external stakeholders. Additionally, the overall framework is assessed and the findings will serve as an input for the first step.

---

[10] As argued by Chernobai et Al. (2006), operational risk measurement techniques can be divided in two main groups: Top-down or Bottom-up approaches. Top-down approaches have the benefit of being relatively inexpensive and easy to implement, while bottom-up approaches are more costly and at the same time more accurate (Marshall, 2001)

[11] The decision of whether to retain or not a risk rests on a simple principle: A corporation should retain all those risk where it has a competitive advantage in managing it, respectively transfer all other risks (Nocco and Stulz, 2006)

Last but not least, in relation to risk management frameworks, often authors relate the concept of bureaucracy. In particular it is argued that risk management practices have increased the bureaucratic burden for corporations (Power, 2004 and 2007). By developing the ideas of Power (2004, 2007), Habib and Chen (2009) have provided evidence that risk management, besides for being bureaucratic, also moralizes organizational life. Additionally, imposed risk management practices are likely to be associated to further bureaucracy as "conformity to institutionalized rules often conflicts sharply with efficiency criteria" (Meyer and Rowan, 1977).

Best practices

Because operational risk involves a broad set of activities and disciplines, it is impossible to summarize best practices as they extent to basically each activity of the bank; from policies regulating anti-money laundering to the security level of the IT system. However, there is one aspect of operational risk that has attracted the attention of researchers and is directly imputable to operational risk management: risk awareness. The establishment of a risk aware culture is considered to be a key element of managing operational risk (e.g. Buchelt and Unteregger, 2004; Rao and Dev, 2006; Moosa 2007).

As argued by Marshall (2001) operational risk management relies on the positive attitudes of staff at every level. Such attitudes can be nurtured by risk aware culture or obstructed by a mere focus on short-term profits. Corporate culture can be defined[12] as "a complex set of values, beliefs, assumptions, and symbols that define the way in which a firm conducts its business" (Deal and Kennedy, 1982; Barney, 1986). Therefore, despite for the intangible aspects of a corporate culture (beliefs), risk policies and standards (norms) can be used to inspire and direct the behavior of employees (Marshall, 2001). Additionally, with regards to corporate culture, a big challenge that financial corporations face is to institutionalize and leverage individual learnings (Marshall, 2001). As business increased in scale and complexity, individuals learn about operational risks before the organization does, therefore financial organizations need to disclose the individual's finding and adapt policies in order to leverage it throughout the corporation (Ibid).

Basel Committee on Banking Supervision (BCBS)

The Basel Committee on Banking Supervision (BCBS) is governed by the Bank for International Settlements (BIS) and can be considered as the most prominent regulator within the financial industry. The BCBS provides a forum for cooperation on banking supervisory matters and promotes financial stability by attempting to avoid systemic failure (BIS, 2010).

[12] For more on the concept of operational culture please refer to Smircich (1983)

The BCBS has two important contributions to the management of operational risk. Firstly, operational risk management is regulated in the Basel II framework (BCBS, 2006). Operational risk is discussed in the first pillar of the framework, i.e. minimal capital requirements. This approach is quantitative and aims at the measuring of operational risk (risk modelling) rather than at improving its management[13]. Secondly, the BCBS recently issued a reviewed version of the "Sound Practices for the Management and Supervision of Operational risk" (BCBS, 2011). The best practices emphasize a qualitative approach by outlining 11 principles of sound operational risk management that address three main issues: governance, risk management environment, and disclosure.

The details of the eleven principles[14] are not presented to the reader as the comprehension of each principle is not a prerequisite for the understanding of the paper. Nevertheless, the comments of Bolton and Berkey (2005)[15] are self-explicatory: "[The] sound practices paper provides an excellent outline for designing an operational risk management framework that can provide tangible benefits and does not get distracted by the challenges of operational risk modelling". Despite the enthusiasm of Bolton and Berkey (2005), because the guidelines have to accommodate the needs of unique financial organizations and are addressed to the highest authorities of the bank, they remain at a broad and conceptual level.

As a conclusion on the frame of reference chapter, it is important to notice that while there is a lot of literature on the conceptual aspects of operational risk and its measurement, the same cannot be said about operational risk management best practices. The financial industry quantitative bias was reflected into its research and best practices have been overlooked. Because operational risk extends to all the disciplines of a corporation (e.g. from abstract concepts such as corporate learning to concrete aspects such as the insurance of employees or the security of the IT system) providing an ultimate reference to operational risk management best practices is extremely difficult (Marshall, 2001). As a result, risk managers at the business unit level don't have a framework or a model to refer to. The general principles outlined by the BCBS (2011) is all they have.

---

[13] The BCBS describes three different approaches that banks can use to define their operational risk capital requirement. 1) The Basic Indicator Approach: Banks using the BIA must hold capital for operational risk equal to the average over the previous three years of a fixed percentage (denoted alpha) of positive annual gross income; 2) The standardised approach: Banks' activities are divided into eight business lines. The capital charge for each business line is calculated by multiplying its gross income by a factor (denoted beta) assigned to that business line. 3) Advanced Measurement Approach: a sophisticated quantitative and qualitative approach to measuring the capital requirement for operational risk (BCBS, 2006)

[14] More information about the 11 principles of the Sound Practices for the Management and Supervision of Operational Risk (BCBS, 2011) is available at the following link http://www.bis.org/list/bcbs/tid_28/index.htm

[15] Based on the first publication of the Sound Practices for the Management and Supervision of Operational Risk – BCBS (2003)

Methodology

Data Collection

The relevant information was gathered through a case study that focused on a single global financial corporation. As claimed by Yin (1984) and Stake (1995), the case study design is suitable to complex researches that focus on a specific subject. In a similar vein, Feagin et Al. (1991) argue that the case study methodology is ideal when a holistic and in-depth investigation is needed.

The study combines different qualitative methods, namely: ethnography, semi structured interviews and documentary collection. A qualitative approach was preferred[16], because attention is devoted to the management of operational risk rather than its measurement[17].

The ethnographical study was carried out at the head quarter of a global European financial institution with more than 50'000 employees. My role was openly communicated across the unit and to avoid information sharing resistance I was internalized through a working contract that allowed me to be perceived as a common employee. A six weeks observation period took place at a control department that governs the risk management issues of a business unit named IA (Investment Advisory). IA is part of the private banking division of the bank and offers investment/portfolio advice[18]. From a risk standpoint, IA can be portrayed as an asset management division where credit and market risk are transferred to the client while operational risk is fully borne by the bank. This implies that all the risks encountered are per default operational.

Additionally, besides for public available documentation such as annual reports, etc. access to the bank's internal documentation was provided. The internal documentation of the bank is divided into three categories: 1) Internal documentation that can be shared with specific external stakeholders, e.g. presentations about the bank's offering, etc.; 2) Internal documentation that is available to all employees; e.g. policies, manuals, standards, etc.; 3) Confidential documentation that is available to a restricted number of internal employees, e.g. loss event reports.

---

[16] However, it should be noted that when discussing some specific features of operational risk, e.g. fat tailed distributions, a quantitative approach was chosen for the collection and analysis of the data

[17] Additionally, as argued throughout the paper there are several limits to applying quantitative methods to operational risk management (Marshall, 2001; Muzzi, 2003; Chernobai et Al., 2006; Rosenberg and Schuermann, 2006)

[18] The advice is offered at different service levels, with distinct investment strategies, and is available to several markets. Depending on the investment requirements of the client and its preferences several service levels are made available; from essential monthly e-mail based recommendations to more sophisticated offerings that include frequent interaction with an investment specialist

Fifteen interviews have been carried out (Appendix: Table 1) on the basis of an interview guide that was modified to suit different groups of interviewees. A first contact with RM1[19] was established and further interviews were arranged through its connections. Such approach to sampling is technically defined as convenience and snowball sampling (Bryman and Bell, 2007). Ethnographic studies and qualitative interviewing are commonly supported by such sampling methods (Ibid). Furthermore, a semi-structured interview method was chosen as it allows for flexibility and the same time it emphasizes the active role of the interviewee in framing and understanding the discussed issues (Bryman and Bell, 2007).

Data analysis

In line with Creswell's (2009) understanding of qualitative data analysis, reflection and interpretation occurred during the process of data gathering. Initially, in order to be able to contextualize the findings at the business level, the analysis of the data started through the examination of external and internal documentation that mainly concerned the whole bank, e.g. annual reports and corporate risk policies. At a second stage, the internal documentation that directly concerned the business unit at hand was analyzed. Thereafter, the interviews took place. The data gathered through the interviews was analyzed and interpreted by writing a report. As important findings emerged they were discussed with RM1.

Ontological foundation

As argued by Habib and Chen (2009), because of the multidisciplinary aspect of operational risk its ontological foundation is hard to define. However, there has been a tendency to conceptualize operational risk in a technical and rational way (e.g. Allen et Al., 2004; De Koker, 2006; Chernobai et Al., 2007). A technical approach to the investigation of operational risk forecloses several learning possibilities (Power, 2004; Habib and Chen, 2009). In order to increase the legitimacy of the paper, besides for the standard rational approach, this study also includes aspects of operational risk that stem from non-financial fields. In particular, an alternative understanding of operational risk is emphasized when suggesting further academic research.

Empirical Findings

Operational Risk

The bank defines operational risk as "the risk resulting from inadequate or failed internal processes, human error and systems failure, or from external causes (deliberate, accidental or natural)"

[19] Please refer to the Appendix table 1 for information about the informants

(Annual report, 2010). While this definition is also shared among the risk community of the bank (RM1, RM2, RM3), managers and investment advisors (BM1, BM2 and IA1) tend to perceive operational risk in a narrower manner by overemphasizing transactional risk.

Operational risk has increasingly attracted the attention of higher management (RM1, RM2). Particularly, it has been stressed that a growing amount of resources have been devoted to operational risk, both on the management side and on a more conceptual level (RM2). As mentioned by RM1, the increased interest in operational risk is the result of regulatory compliance. However, as pointed out by a senior manager, the regulatory interest in operational risk was the result of radical changes in the industry:

> *"Viewing the increased interest in operational risk as the result of regulatory requirements is quite limited […] regulators always react to changes within the environment […] operational risk became of interest because of IT developments and other trends within the industry […] as volumes and complexity increased, the game got more sophisticated" – BM1*

Today, as a reaction to the financial losses and reputational damage that banks faced in 2008-2009, risk management practices are in the spotlight as executive members' risk aversion increased (annual report, 2001-2010). In the light of the increased risk aversion, operational risk management can be considered part of the bank's core activity (Internal document, 2011). Additionally, while the risk community of the bank does not understand operational risk as one-sided (RM1, RM2, RM4):

> *"Reducing operational risk not only implies spending money to set up a new framework or control process, it also implies affecting transaction volumes, speed to market, etc. […] it has an impact on the bank's revenues […] It cannot be seen as one-sided" – RM2*

Business managers (BM1; BM2) indirectly state the opposite:

> *"My concern is to get rid of it* [operational risk]… *Possibly in the most efficient way" – BM1*

Operational risk management at the corporate level

The bank has developed five key principles that set the foundation of all risk related activities: 1) Risks are consolidated and assessed at a group level; 2) All employees are involved in the management of risk; 3) Management is accountable for risk; 4) Risk management is monitored by an independent control function; 5) Risk information is disclosed (Internal document, 2011). From a governance perspective, it is noticeable how middle/lower management is responsible for the execution of the risk management activities (Figure 2):

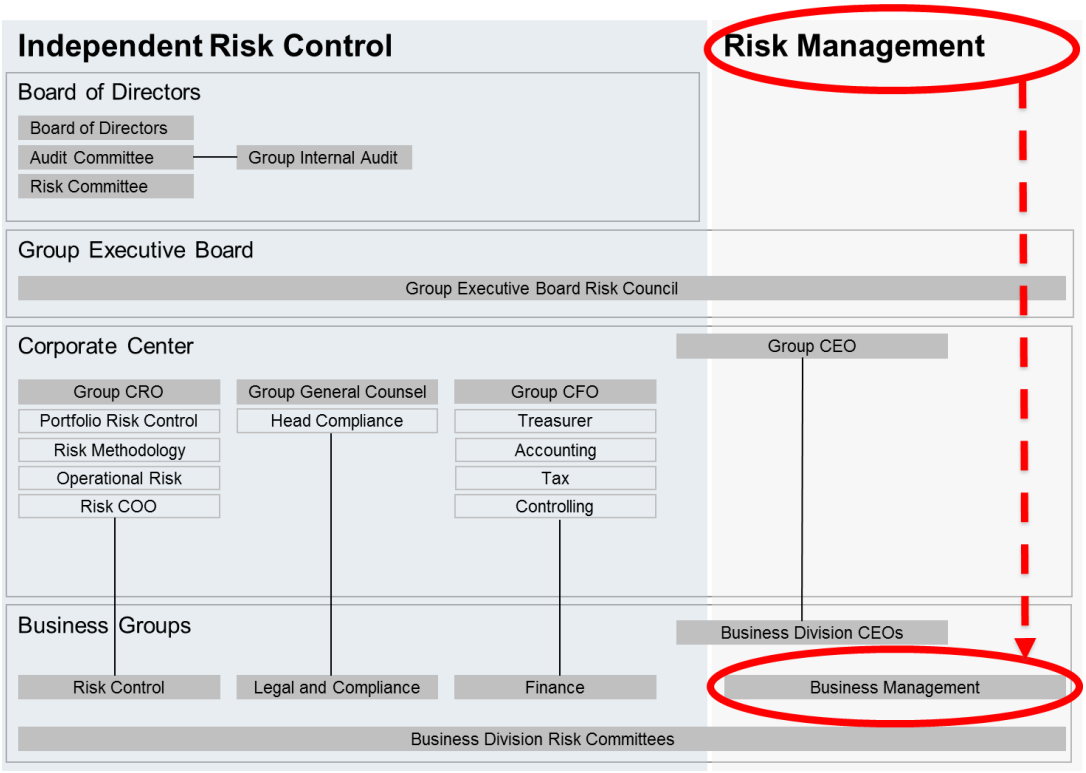

Figure 2: Risk Control and Risk Management – Source: Annual Report 2010 (Reinterpretation)

To promote a sound management of operational risk, the bank has developed an ORF – Operational Risk Framework (Internal Document, 2011). The ORF (figure 3) relies on three key principles: 1) Management is responsible for operational risk; 2) Operational risk management is independently monitored; 3) A cost-benefit analysis is always carried out before taking remedial actions.

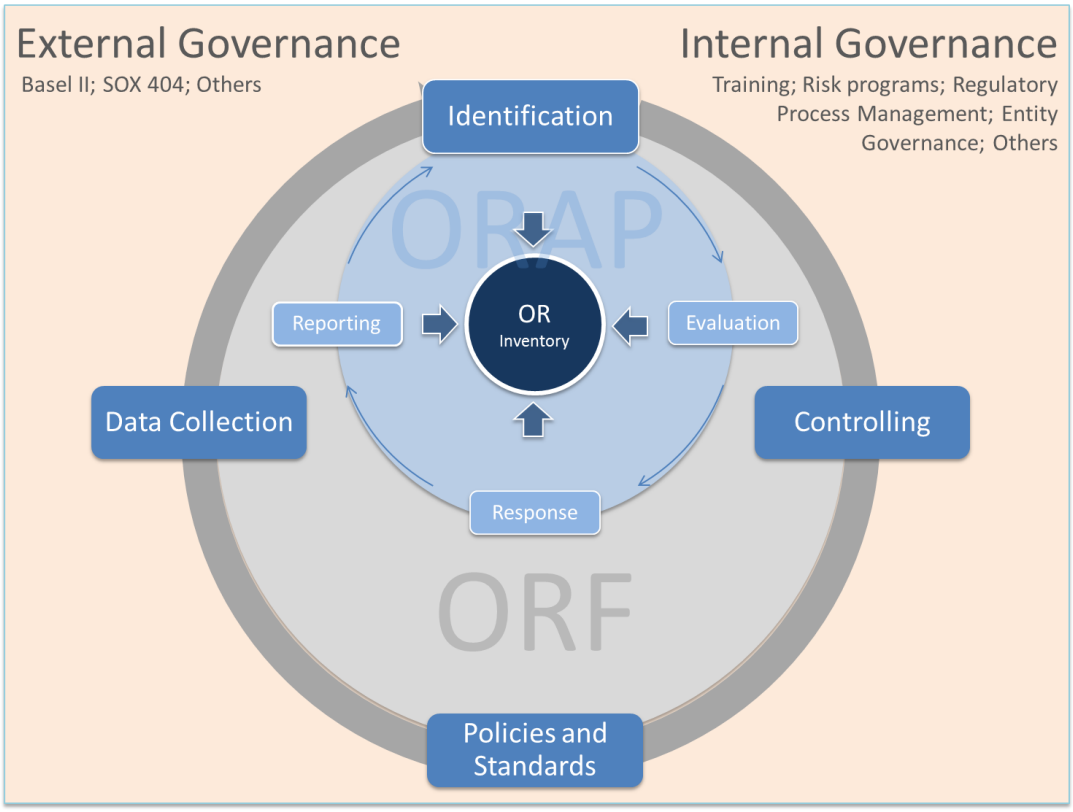

Figure 3: Operational Risk Framework - Source: Internal Document (Reinterpretation)

The ORF does not limit itself to regulating the actions of operational risk management but is a more encompassing model that links the management of operational risk to the overall strategy of the bank and its risk framework. The execution of operational risk management is carried out through the Operational Risk Assessment Process and will be described from the business unit perspective.

Risk culture

As part of the overall risk management framework of the bank, in 2008 a global program was launched with the objective of promoting a risk aware culture across the organization (Internal Document, 2011). The program is resource-intensive and characterized by 14 diverse and multidisciplinary actions (from improving risk policies to addressing the product suitability of the bank). The different actions aim at the whole corporation and as of today the program is still on going. Through on-line courses, risk policies, and reviewed business practices the bank promotes clear risk governance, accountability and control. As stressed throughout all the interviews, the program was effective as all employees can be defined risk aware:

> *"Risk is important. Higher management is really concerned with it... It's not something they will close an eye on" – BM2*

> *"Risk has been on the agenda of management for a while. I can't recall how many training sessions I had since I started to work here" – IA2*

In particular, employees highlighted that besides for several risk training courses, the introduction of risk criteria in the individual performance evaluation established a strong consideration for risk. Approximately 20% of the employee's performance evaluation is based on risk criteria such as "I will strictly comply with the risk policies relevant to my role. I will record all mandatory information and update it regularly" (Internal document, 2011). Being that the variable compensation of employees (bonus) is dependent on their individual performance evaluation, it does not come as a surprise that employees are concerned with risk management best practices.

Operational risk management at the business unit level - IA

QRM (Quality and Risk management) manages operational risk for IA (Investment Advisory). Besides for taking care of the daily risk related issues, QRM also ensures that risk policies are effective and promotes its enforcement. However, the ultimate responsibility for operational risk rests within the business function (IA) and therefore managers monitor and approve QRM's activity.

Figure 4 provides a simplified overview of the governance of operational risk at IA. The visual representation is QRM centric, i.e. it highlights the main interactions and relations of QRM but does not show how other units interact with each other, nor it represents the different hierarchical levels of the discussed units/functions.

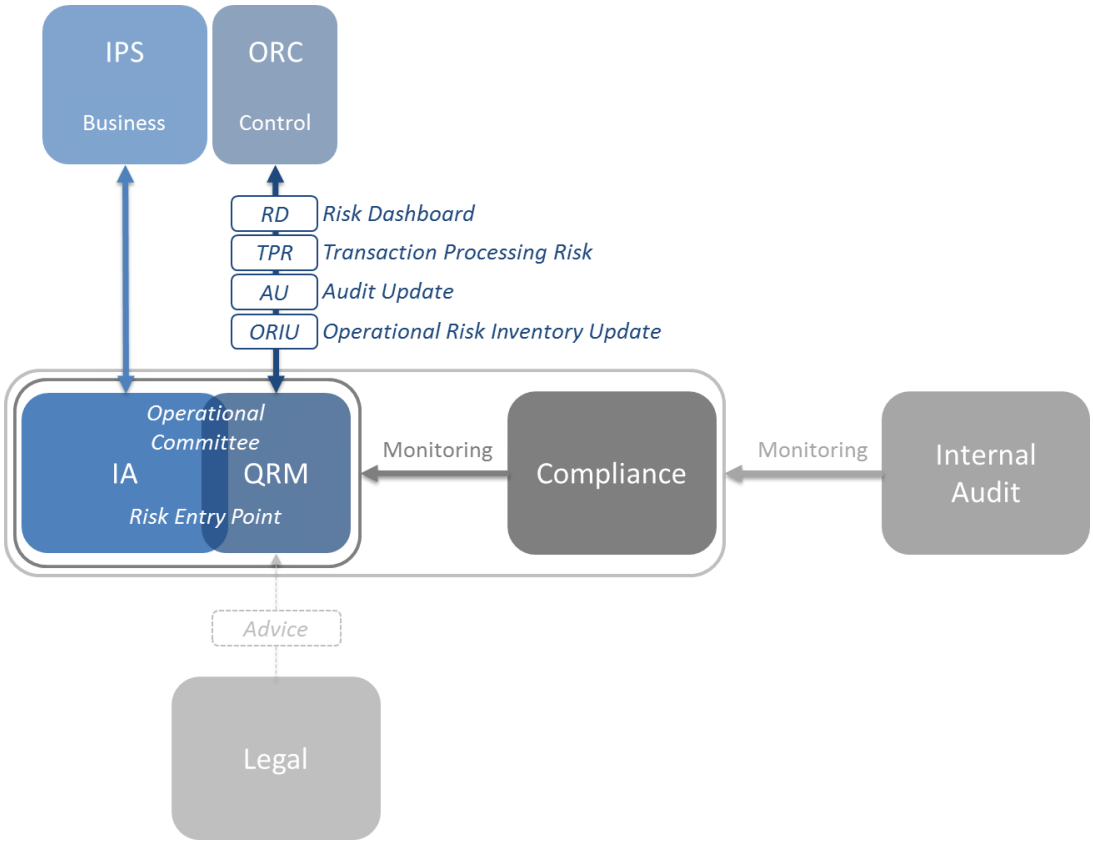

Figure 4: Governance of Operational Risk at IA

QRM has a dual reporting line; it reports to the head of IA and to a higher control function (ORC)[20]. However, because QRM is evaluated by the business function rather than the control function it should not be understood as a compliance oriented "police officer" but rather as a business enabler with a strong sense of urgency for risk matters:

> *"QRM is definitely a business partner; they are not like audit" – IA2*

Identification, Assesmen, Response, and Reporting

Before starting with describing the risk management process, it should be noted that risk management practices are by far less formal than how suggested in policies. Risk managers go beyond their official responsibilities through a set of unstructured interactions. For example, whenever RM1 encounters a risk that might be faced by another unit, such unit is contacted. While

[20] It should be noted that the link to the higher control function is not direct but reached through a COO function.

this might appear as common sense, the example highlights the limits of understanding risk management practices through policies and regulations:

> *"Internal policies only represent the tip of the iceberg of our activity…" – RM1*

Identification – Key interaction: QRM and IA employees

The identification process starts with the definition of a comprehensive ORT (Operational Risk Taxonomy). The ORT defines the universe of inherent material operational risk on an event-based criteria. At a first level, 13 operational risk categories are identified which are further broken down in to 30 sub-categories[21]. Thereafter the actual risk identification process takes place. At IA the identification of risk is the result of the interaction between QRM and IA employees:

> *"If something goes bad, QRM is directly informed" - IA1*

QRM can be described as the "entry point" for all risk related issues; i.e. when a risk event is about to, or already materialized the investment advisors contacts the QRM department for guidance. Therefore, when it comes to identifying risks, IA strongly relies on the input of investment advisors. Throughout the interviews with RM1, RM2, BM2, L1, IA1, and IA2 transactional risk; cross-boarder risk; and product suitability risk emerged as the most important risks for the unit.

Last but not least, it was evinced that the interaction between QRM and IA employees is extensive and supported by physical proximity:

> *"Having my office next to them is perfect […] it facilitates the interaction as investment advisors are free to drop by whenever they need to" – RM1*

Also, interaction is encouraged through business embeddedness:

> *"It really helps that QRM is on our side, it's not like talking to a police officer […] They understand our need for business […] it motivates you to talk with them" – BM2*

Evaluation – Key interaction: QRM and ORC

Once risks have been identified, their assessment is based on its severity and frequency. The severity of an operational risk is ideally defined on its financial consequences, however this is not always possible. Therefore, the evaluation of the severity of an operational risk might be based on an estimation of the reputational damage or regulatory sanction that might be inflicted to the bank

[21] The identified risk categories of the bank can be considered a reinterpretation of what outlined in Basel II – Annex 9 – Detailed Loss Event Type classification (BCBS, 2006)

(internal document, 2011). As a result of the assessment, operational risks are sorted in one of the three magnitude-based categories: green, amber and red.

The assessment of the different risks faced by IA is carried out by QRM with the support of ORC. As highlighted in figure 3, the interaction between QRM and ORC is institutionalized through four main risk tools. For the purpose of this paper, the analysis is limited to the RD (Risk Dashboard) and the TPR (Transaction Processing Risk).

The RD is a risk tool that serves to collect all the operational risks faced by the business unit. For each risk category QRM is required to enter the identified risks, describe and assess them. For example, if the risk manager is informed that the only French-speaking member of the business unit resigned, he will do an entry under the "employment related risk". The risk manager will assess the risk as "green" because he knows that management is already interviewing two different candidates and therefore the risk that the unit might not be able to offer its services to the French speaking clients is limited.

Despite for the absence of a financial indicator, what makes the risk manager's task of assessing (quantifying) risks particularly troublesome is the absence of measurable features:

> *"I spent almost 2 hours trying to assess the consequences of a fee miscalculation for a group of clients […] at the end the assessment of the risk was based on my gut feeling" – RM1*

On the other hand, some operational risks present easily quantifiable metrics and lead to clearly identifiable financial events (losses/gains). For example, transactional risk can be monitored through the volumes of trades, the number of trades per investment advisors, etc. Additionally, transactional risk has clearly quantifiable economic consequences. According to the monthly TPR report at IA transactional risk events averaged gains/losses of EUR 5'000, while peak events exceeded the EUR 150'000 threshold. Additionally, it was observable that the number of errors is particularly low:

> *"We hired an external consultant to try to improve the loss-events/trades ratio. After presenting him the figures of the unit, the consultant asked me – "why did you hire me? It seems like your guys are doing a great job, let me see, give or take they miss one trade every three thousand… Last week I was working with an airline company that is not able to deliver the customer's luggage five times every hundred…" – that is when we realized that no matter how good you are, risk is part of the business and you will have to accept it" – BM1*

Last but not least, as financial events take place, they are registered in a database. The inputs are consolidated by a higher control function and shared back with the unit (TPR report). The database provides with detailed information about how the financial event happened and which remedial actions have been taken. The financial events that take place in other units are usually not discussed and as a rule managers do not share such details with employees.

Response – Key interaction: QRM, QRC and IA

Once the RD is filled out, a higher control function (ORC) consolidates the risks of all different units. For each risk category, the consolidated risk assessment is matched against the risk appetite of the bank. As a result, the ORC establishes whether the current risk exposure is below, in line, or above the agreed risk appetite. Thereafter, the consolidated analysis is shared back with the business units and serves to provide guidance and sense of urgency for each specific risk that the individual business units face. For example, the regulator of a country has changed a policy that affects 10 clients of IA. Because IA will need some time to comply with the new regulation, a risk entry is done in the RD. The risk manager will rate the risk green as only 10 clients are affected. However, at a consolidated level 500 clients might be affected. As a result the ORC will change the risk rating to red in order to insure that the risk is a priority on the agenda of individual risk units.

On the basis of the risk assessment, the IA OC[22] (Operational Committee) has to determine whether the response should be mitigation or if the risk should be accepted. If the risk is accepted, a dispensation has to be requested[23]. On the other hand, if the bank decides to mitigate the risk, an action plan is defined. As discussed with RM1, RM2, and RM4 mitigation issues mostly concern amendments of policies. However also halts of business might be imposed. The IA OC should not be seen as a forum for risk discussions but rather as a meeting where previously discussed risk issues are endorsed:

> *"If you want to get something approved by the OC, you cannot just show up and ask the members about their opinion on it. You need to call them up in advance and make sure that relevant members of the committee understand your issue and proposed mitigation measures. There is not enough time […] The OC is the place where decisions are made and confirmed. Only to a lesser extent, issues are discussed […] It's where our activity is formalized" – RM1*

[22] The OC is made up of members from different divisions of the bank (IA management, QRM, ORC, business development, etc.) and institutionalizes the risk management activity that takes place during the daily activity of QRM

[23] Depending on the assessment of the operational risk (green, amber, red), approval for dispensation will require higher corporate authorities to sign-off the authorization

Reporting and monitoring – Key interaction: ORC, Compliance and Audit

This last step consists of delivering risk stakeholders with information and assessing the reliability of risk practices. It is mainly carried out by the ORC, Compliance and Audit.

A reactive process

The risk identification process is a reactive process rather than a proactive practice:

"They will come to us too late, once it has already hit the fan" – L1

Although operational risk management practices react to several events, it was observed that they are mainly influenced by monetary losses or quasi-losses. For example, as discussed with an investment advisor (IA2), while the dealing of option orders is per definition more complex and therefore subject to a greater risk of mishandling than plain equity trades, management waited until losses[24] took place before applying tighter control procedures:

"It doesn't take a rocket scientist to figure out that trading errors are more likely to occur for option trades than for equity trades. Yet, management waited until several financial events took place before introducing the four eyes control principle" – IA2

Investment advisors and risk managers have provided other examples of this dynamic, from cross boarder activities to other typologies of trades (e.g. forward currency trades). The common denominator of the examples is that the bank has a reactive stance to financial events. The question that follows is why? Why is operational risk management a reactive process rather than more compelling forward-looking practice? According to RM1 one has to keep in mind that resources are scarce and even if potential risks are identified, the bank cannot control for all of them:

"If I was to write down all the potential risks that the unit might face I would spend the whole day by filling up the risk dashboard, but then what do you do with that information? If I know that there is no room for action I will not mention the risk. For example, there is little need for constantly rethink and report the risks of the current IT set up if you can't constantly change it. The same goes for HR related risks; there is always the risk that a key employee will leave, yet there is little added value if this is constantly reported […]the unit will have to live with the fact that risks will always exist" – RM1

[24] It would be more appropriate to talk about financial events (rather than losses) as transactional risk can lead to both profits and losses. However, through an internal scheme, financial events that lead to a profit are usually not captured by management as the investment advisor allocates the gains to the client or the trader in order to not report the error.

In the light of what stated above, management and risk management learn from financial events and eventually decide to tighten the current procedures (e.g. by requiring an additional control step). However, as discussed with the uppermost manager of the unit, not all financial events have the same learning impact. For example, a typo mistake or a breach of the internal trading policies has a learning impact that is limited to the person incurring in the mistake. On the other hand, a mistake that leads to a change of business practices has an extended learning and affects the whole unit.

Bureaucracy

Operational risk management was often associated to the issue of bureaucratization:

> *"If you really want to track and monitor all the activity of a risk manager, you end up wasting more resources in documenting and analysing what you are doing rather than focusing on potential risks" – RM1*

> *"A list for this, a list for that […] the costs of risk reporting are enormous. I understand that they need to know what I do, yet I have to spend time in meetings and filling out lists when I could be working on something that really has an impact […] It almost feels like risk management didn't change that much in the past 5 year. What really changed is the amount of resources devoted to describe and disclose our activity […] Today, legal and compliance has head-locked the whole bank […] we have taken the lead in business. You can't do anything without our approval" – L1*

Additionally, as highlighted by a manager, a risk aware culture has multiple benefits but at the same time, it promotes bureaucracy across the organization processes:

> *"A risk aware corporate culture is a good thing per se, however the bank has to be careful. If the employees feel like the bank is transferring the corporate risk responsibilities on them, than the functioning of the bank might be jeopardized as all employees apply internal policies rather than common sense" – BM1*

In particular the manager was referring to the fact that, as part of the risk aware cultural program that was started in 2008, today each employee's performance is also evaluated on risk criteria.

Discussion

Operational risk

The definition of operational risk adopted by the bank is aligned with the BCBS (2006). This confirms the wide usage of the definition provided by the regulator. However, despite the corporate

recognition of the definition, among its employees only the risk community was familiar with it. This highlights that operational risk understanding can be improved.

In line with the literature (e.g. Hussain, 2000; Chernobai et Al., 2007; Halperin, 2001), evidence was found that as a result of trends within the financial industry and because of regulatory compliance (BCBS, 2006), the bank is concerned with operational risk. Nowadays, managing operational risk can be considered as part of the core activity of the bank (Internal document, 2011).

Additionally, the collected data provides interesting insights to the conceptual aspects of operational risk: First, operational risk is considered to be diverse and multidimensional (Milligan, 2004; Buchelt and Unteregger, 2004). Because the risk taxonomy of the bank includes more than 30 risk categories, the diversity feature of operational risk emerged constantly. This feature manifested throughout discussions with risk managers, business managers and investment advisors. Second, the fact that operational risk lacks a financial indicator (De Koker, 2006) was also confirmed. Referring to the difficulties of assessing operational risk, RM1 emphasized the lack of quantifiable data. Third, transactional risk events averaged gains/losses of EUR 5'000, while peak events exceeded the EUR 150'000 threshold. Therefore it can be concluded that operational losses are characterized by a fat tail distribution (Chernobai et Al., 2006). Fourth, regarding operational risk management as a cultural issue refers to the fact that it cannot be retained by management (Buchelt and Unteregger, 2004). Such a feature was confirmed by the launch of a global program that aimed at promoting a risk aware culture and by the fact that each employee is responsible for operational risk.

The gathered evidence confirms that operational risk is diverse; lacks a financial indicator; features a heavy tailed distribution; and can be considered a cultural issue. However, the endogenous feature (Kaiser and Kohne, 2006) is rejected. Two out of the three main risks that IA faces (cross-boarder risk and product suitability risk) entail a prevailing component that is external to the control of the bank (regulatory compliance). Additionally, the recent natural disaster that took place in Fukushima (Japan), reminded the world in the most sorrowing way that operational risk can originate from the external environment.

As to be expected, finding answers to the debated features of operational risk is not straightforward. The debate on whether operational risk is to be considered as a one-sided risk is not settled. In line with Moosa (2007), there is absolutely no doubt that viewing operational risk as a downside or one-sided is erroneous and this view was confirmed by RM1, RM2 and RM4. However, throughout the interviews business managers confirmed the views of Herring (2002) and Crouchy et Al. (2004) by stating the opposite. The question is why?

If managers really believed that operational risk is one sided why aren't they acting accordingly; i.e. if management was to believe that operational risk is one-sided, they should implement policies aiming at completely avoiding operational risk. For example, they could make it mandatory to have a 20 eyes control principle on each trade. This is not done because the opportunity cost of such action is too high, i.e. efficiency ratios such as number of clients per investment advisor would quickly drop in order to accommodate the new risk procedures. This implies that operational risk is not one-sided… Thus, the study shows that by introducing the concept of efficiency management does not view operational risk as one-sided, that is – one should look at what managers do, not what they say.

Since operational risk is easier to understand as one-sided risk (Moosa, 2007) and because managers are paid for managing it rather than defining it, they are not concerned with its conceptual definition. A possible explanation to the fact that managers erroneously view operational risk as a one-sided, can be imputed to a lack of reflection. However, further research is required to better understand the discrepancy between their statements and their actions. In particular, this inconsistency could be clarified by approaching the analysis of managerial behavior through the lens of the bounded rationality theory (Herbert, 1955).

The study was carried out at a business unit that faces operational risks only, therefore the two remaining debated features of operational risk couldn't be confirmed or rejected. However, as discussed during the literature review, from a theoretical perspective there are more arguments for rejecting rather than accepting both features. In order to find answers on the idiosyncratic proposition (Lewis and Lantsman, 2005) a quantitative research that is not limited to a single financial organization would be required. On the other hand, to confirm or reject the indistinguishable feature of operational risk (Buchelt and Unteregger, 2004), a study should be carried out at the corporate level.

Operational risk management

As a starting point it can be noted that risk management theories and practices, in line with economic thinking, are biased towards an ultra-rational understanding of corporations. In order to simplify complex processes and networks of interactions, regulators, academics and practitioners have a mechanistic conception of the corporation. In reality, as stressed throughout an analysis at the business unit level, risk management practices extend further beyond the limits of formal displays.

At a corporate level, with particular emphasis on the operational risk framework, it is noticeable how the bank has implemented the recommendations outlined by the regulator (BCBS, 2011). This confirms that regulators aim at the corporate level and signals that they do it effectively. Additionally, because operational risk is multidisciplinary (Marshall, 2001), the bank approaches operational risk from a broad perspective that includes business standards, risk policies, and controlling procedures. This aspect was further emphasized by the launch of a corporate program that aimed at establishing a risk aware culture that extends to all the divisions of the bank.

At the business unit level, the general model for operational risk management (identification, assessment, response, reporting and monitoring – e.g. Bessis 2010) was reflected in the bank's practices. Also, despite risk tools and sense of urgency provided by the top-down approach, it was observed that no concrete input is given in relation to the how to deal with the daily risk activities.

The little guidance that risk managers get at the business level led to the emergence of a pragmatic and reactive process where responsibilities between business and control functions are blurred. Additionally, the overall risk management practice was often related to the problematic of bureaucracy. In the following sections the key findings that emerged at the business level are developed and further academic research is suggested.

Governance and independence

At IA operational risk is management's responsibility, however in practice QRM manages operational risk. In other words, middle and lower management limits itself to approving and monitoring the actions of the risk management function rather than actively engaging in such activity. According to the information disclosed to shareholders (annual report, 2010), this should be the other way round (figure 1). However, before erroneously concluding that managers are not fulfilling their risk duties, it has to be noted that managers are responsible for risk not for the execution of its management (BCBS, 2011). Manager base their risk decisions on the analysis carried out by risk specialists. The question that follows is: why can't risk managers be responsible for the risks of the bank? The answer is straightforward; there would be a clear conflict of interest. While managers aim at balancing risks and revenues (Bessis, 2010) risk managers would simply attempt to avoid exposure as they have downside potential only.

Because QRM is evaluated by IA rather than ORC, viewing it as an independent control function is inappropriate. As highlighted by managers and investment advisors, QRM is perceived as a business partner rather than an exogenous compliance officer. As a consequence of gaining business embeddedness, QRM also loses its independence.

At a first glance this might sound alarming as regulators constantly stress the importance of the independence of risk management (BCBS, 2011). However, the independent status of the control function is re-established at a higher hierarchical status and through the actions of Internal Audit, Legal, and Compliance. Moreover, because risk managers are not perceived as exogenous compliance officers, a positive, trustworthy and commitment based relationship is established. Strong interaction between risk managers and investment advisors is important because employees are key source for the risk identification process (Marshall, 2001). Therefore, business embeddedness emerged as a critical feature for the successful management of operational risk at IA.

However, as stressed by regulators business dependence brings along the threat that risk managers "partner up" with business managers and focus on revenues only (Bessis, 2010). Therefore, besides for specific technical capabilities, it is important to ensure that risk managers are also guided by the right visions. This last aspect leads to another interesting consideration; at the business level, the quality of risk management doesn't depend on the corporate risk framework but rather on the contribution and motivation of individual risk managers.

Operational risk as a reactive process

Although operational risk management practices react to several events, evidence was made available that risk management is mostly influenced by monetary losses or quasi-losses (RM1, RM2, IA1, IA2, BM1, BM2). The process of managing risk can be understood as a sophisticated trial and error process where every time that a monetary loss or quasi-loss takes place, in order to prevent it from happening again, policies, manuals and procedures are modified into a more fine-grained and sophisticated system of rules. Therefore, the management of operational risk can be represented as a cognitive process where each business unit learns from specific events and as a result risk practices are adapted/improved.

By analyzing the option-dealing example it is clear that management's reluctance to tighten control procedures stems from efficiency concerns (Marshall, 2001). However after several losses manifested, managers decided to implement a more sophisticated policy, the four eyes control principle. This is intriguing because even before the financial events took place, management was aware of the fact that option trades were more exposed to transactional risk. Management needs a justification for lowering the efficiency of the unit through additional control procedures (Ibid).

Indirectly this implies that a forward-looking analysis might not be a strong enough argument to win the conflict that exists between control and efficiency[25].

As introduced by RM1 and BM1, the unit has to accept that risk is part of business. As argued in the most basic financial theory, if the bank was to the eliminate all its risk, shareholders, in return for their capital would get the risk free rate (Elton and Gruber, 1995). Therefore, implementing mitigation actions to each potential risk is not an appropriate solution. Additionally, following Nocco and Stulz's (2006) strategic rationale, banks have to maintain exposure to operational risk because they are particularly good at managing it (BM1). In this context, given that the current risk management policies are solid, a reactive stance to loss events emerges as pragmatic and efficient way of identifying risks.

Cognitive processes are hard to be institutionalized into risk management best practices. As argued by Marshall (2001), because not all individual learnings are extended to the unit, tacit knowledge is developed. Although individuals learn the most when directly involved with operational risk events (IA1, IA2 and BM1), it is suggested that individuals sharing their experiences can extend the reach of their learning to the group (Marshall, 2001). Therefore, the unit could increase operational risk management capabilities among its employees by sharing risk information that is currently limited to management. This conclusion is based on intuition and could gain credibility by being further researched through the lens of organizational learning[26], and the concepts of single and double loop learning[27].

Bureaucracy

Throughout the interviews, operational risk management was often associated to the issue of bureaucratization (Power, 2004 and 2007). This is understandable because the operational risk framework is conceived at the corporate level, i.e. its requirements are imposed on the business unit and they make sense only at a higher level.

While bureaucracy is part of each global corporation (Power, 2004), an over-bureaucratization of risk management processes is to be avoided as it hinders the efficiency of processes (Marshall, 2001). Controversially, as highlighted by a manager, a risk aware culture has multiple benefits but also promotes bureaucracy across the organization processes. In particular, the introduction of risk criteria in the performance evaluation of each employee might encourage investment advisors to

[25] Here as well, managerial behavior could be approached through the theory of bounded rationality (Herbert, 1955).

[26] For an overview of organizational learning please refer to Dodgson (1993)

[27] The notion of single and double-loop learning arise from Argyris and Schon's theory of action (Argyris and Schon, 1978)

engage in "cover your back activity" (e.g. getting approval for each single transaction from QRM, Legal or Compliance) rather than performing revenue generating business duties (e.g. calling the clients, reviewing portfolios, etc.). This kind of attitude has costly consequences for the bank as the overall functioning of the bank is hindered.

Additionally, besides for the burden of the "cover your back" principle, an overly risk aware corporate culture can have even more worrying outcomes at a higher level. Any corporation that is overly concerned with risks might lose its focus on the core business (Marshall, 2001). As highlighted by L1, the legal and compliance department have "head-locked" the whole bank. This is troublesome because even if managing operational risk is considered part of the core activity, resources have to be devoted to those activities that increase revenues rather than avoiding losses. Therefore, if management's priority converts to risk management, business opportunities might be missed out. At the end of the day, managers have to pursue new business opportunities by identifying those projects that generate a positive return, not prioritize risk mitigation.

As conclusion, while promoting a risk aware culture, practitioners should pay attention to not over emphasize risks (Power, 2004 and 2007). An appropriate balance between risk and business should be pursued. Additionally, from an academic standpoint, further attempts to analyze the current risk management hype through the lens of sociology could be done by applying the new institutional theory developed by Meyer and Rowan (1977) and DiMaggio and Powell (1983). The societal forces that stimulate financial organizations' concern for risk could also provide valuable insight on the problematic of bureaucratization. As argued by Meyer and Rowan (1977), conformity to institutionalized rules conflicts with efficiency criteria. By approaching risk management through such research, evidence might be found that shareholders' need for risk management disclosure is a value destroying activity.

Conclusion

Operational risk

Evidence was found that the financial institution perceives operational risk as a first priority risk by considering it as part of their core activity. Additionally, the research found out that the bank adopts the definition of operational risk provided by the regulator. On a more conceptual level, the gathered evidence led to confirm that operational risk is diverse; lacks a financial indicator; features a heavy tailed distribution; and can be considered a cultural issue. However, the proposition that operational risk is endogenous was rejected.

Additionally, the debate on whether operational risk is one-sided that takes place in the literature was also encountered at the bank. It was concluded that from a theoretical perspective, and with the support of the risk community of the bank, operational risk cannot be seen as one-sided because such view fails to account for the "revenue-side" of the distribution. Additionally, by observing managerial actions it can be concluded that operational risk is not one-sided. However, because management stated the opposite, the debate could not be ultimately settled.

Operational risk management

At the corporate level, it was noted that the bank has implemented the recommendations outlined by the regulator. Also, in line with what is suggested in the literature, the bank approaches operational risk from a broad perspective that includes several disciplines. Additionally, through the analysis of operational risk management at the business unit level, the research demonstrated that understanding operational risk practices through formal displays and technical approaches provides a limited and distorted understanding of such practice.

At the business unit level, it was proved that besides little internal support, managers have no regulatory guidance or theoretical framework to refer to. As a result operational risk management emerged as a pragmatic and reactive process. Although operational risk management practices reacted to several events, evidence was made available that risk management is mostly influenced by monetary losses or quasi-losses. Thus, the process of managing risk can be understood as a sophisticated trial and error process where every time that a monetary loss or quasi-loss takes place, policies, manuals and procedures are modified into a more fine-grained system of rules. Although at a first glance a reactive approach might appear less compelling than a forward looking model, given that risk management policies are solid, a reactive stance to loss events emerged as a pragmatic and efficient way of identifying risks.

The study also shows that at the business level the boundaries between the risk control function and management are somewhat blurred. While the independence of risk managers is an essential condition for regulators, evidence was found that business embeddedness is a critical feature for the successful management of operational risk at IA. However, the paper does not suggest that risk management should be business embedded, in the specific case such feature had a positive contribution because other units ensured the independence and soundness of the overall control framework (e.g. Legal and Compliance, Internal Audit, etc.). Last but not least, at the business level, the quality of risk management doesn't depend on the corporate risk framework but on the contribution and motivation of individual risk managers.

Finally, since the operational risk framework of the bank is conceived at the corporate level, its requirements at the business unit level are often associated to the issue of bureaucracy. Bureaucracy was also associated to a corporate aware culture. While it is suggested that corporations should pursue a risk aware culture, evidence was found that a corporation that is overly concerned with risk might incur in additional bureaucracy and perhaps even greater strategic troubles.

As a concluding remark, because operational risk is multidimensional the focus of regulators on the highest authorities of financial corporations appears as an obligation rather than a choice. The same argument holds for the current academic literature. Given the diversity of operational risk and the dimensions that its management encompasses, framing operational risk management is, at best problematic and at worst impossible. That is why researchers have overlooked best practices by focusing on quantitative approaches. Therefore, it can be concluded that best practices at the business unit level will most likely continue to be characterized by little regulatory guidance. Depending on the different risks that managers encounter, they will have to draw from the research of the specific fields.

Appendix

Code	Time	Title	Role	Internal Role
RM1	4.5h	Executive Director	Risk Manager	Head QRM
RM2	1.0h	Executive Director	Risk Manager	Head IPS ORC
RM3	1.0h	Executive Director	Risk Manager	IPS ORC
RM4	1.5h	Executive Director	Risk Manager	Global Head AM ORC
BM1	0.5h	Managing Director	Business Manager	Global Head IPS IA
BM2	1.5h	Executive Director	Business Manager	Regional Team Head IPS IA
L1	1.0h	Executive Director	Lawyer	Head IPS Legal
CO1	1.0h	Director	Compliance Officer	IPS Compliance
IA1	1.5h	Authorized Officer	Investment Advisor	IPS IA
IA2	1.5h	Director	Investment Advisor	IPS IA

Table 1: Interviews Overview

References

Allen L., Boudoukh J. and Saunders A. (2004), *Understanding Market, Credit, and Operational Risk: The Value at Risk Approach*, Oxford: Blackwell Publishing

Argyris C. and Schon D. A. (1978), *Organisational Learning*, Massachusetts: Addison Wesley, Reading

Bali T. and Allen L. (2007), Cyclicality in Catastrophic and Operational Risk Measurements, *Journal of Banking and Finance* 31, Pp. 1191–1235

Barney J. B. (1986), Organizational Culture: Can It Be a Source of Sustained Competitive Advantage? *The Academy of Management Review*, 11:3 Pp. 656–665

BBA (2000), Operational Risk Management – The Next Frontier, *Journal of Lending and Risk Management*, March, Pp. 38–44

Bessis J. (2010), *Risk Management in Banking*, Chichester: John Wiley & Sons

BCBS (2001), Working Paper on the Regulatory Treatment of Operational Risk, http://www.bis.org

BCBS (2003), Consultative Document: Sound Practices for the Management and Supervision of Operational Risk, http://www.bis.org

BCBS (2004), Bank Failures in Mature Economies, http://www.bis.org

BCBS (2006), International Convergence of Capital Measurement and Capital Standards, A revised Framework – Comprehensive Version, http://www.bis.org

BCBS (2011), Consultative Document: Sound Practices for the Management and Supervision of Operational Risk, http://www.bis.org

BIS (2010), Annual Report 2010, http://www.bis.org

Blunden T. (2003), *Scoreboard Approaches, Operational Risk: Regulation, Analysis and Management*, London: Prentice Hall-Financial Times, Pp. 229–240

Bolton N. and Berkey J. (2005), *Aligning Basel II Operational Risk and Sarbanes – Oxley 404 Projects*, Operational Risk: Practical Approaches to Implementation, London: Risk Books, Pp. 237–246

Buchelt R. and S. Unteregger (2004), *Cultural Risk and Risk Culture: Operational Risk after Basel II*, Financial Stability Report 6

Bryman A. and Bell E. (2007), *Business Research Methods*, Oxford University Press

Cline W. R. (2010), *Financial Globalization, Economic Growth, and the Crisis of 2007-09,* Washington, DC: Peterson Institute for International Economics

Chernobai A., Svetlozar R. T. and Fabozzi F. (2007), *Operational Risk: a Guide to Basel II Capital Requirements, Models, and Analysis*, Hoboken, NJ: John Wiley

Creswell J. W. (2003), *Qualitative procedures, Research Design: Qualitative, Quantitative, and Mixed-Methods Approaches,* Thousand Oaks: Sage Publications, Pp. 179 –207

Crouchy M., Galai D. and Mark R. (2004), Insuring versus Self-Insuring Operational Risk: Viewpoints of Deposits and Shareholders, *Journal of Derivatives* 12, Pp. 51–55

Cummins J. D., Lewis C. M. and Wei R. (2006), The Market Value Impact of Operational Loss Events for US Banks and Insurers, *Journal of Banking and Finance* 30, Pp. 2605–2634

Danielsson J., Embrechts P., Goodhart C., Keating C., Muennich F., Renault O. and Shin H. S. (2001), An academic response to Basel II, *LSE Financial Markets Group, an ESRC Research Centre Special Paper Series*, May

De Koker R. (2006), *Operational Risk Modelling: Where Do we Go from Here?* The Advanced Measurement Approach to Operational Risk, London: Risk Books

Deal, T. and Kennedy A. E. (1982), *Corporate cultures*, Reading, MA: Addison-Wesley

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

Dodgson M. (1993), Organizational Learning: A Review of some Literatures, *Journal of Organization Studies*, 14:3 Pp. 375–94

Doherty N. A. and Smith C. W. (1993), Corporate Insurance Strategy: The Case of British Petroleum, *Journal of Applied Corporate Finance*, 6 Pp. 4–15

Elton E. J. and Gruber M. J. (1995), *Modern Portfolio Theory and Investment Analysis*, 5th ed., New York: Wiley

Feagin J., Orum, A. and Sjoberg G. (1991), *A case for case study,* Chapel Hill, NC: University of North Carolina Press

Halperin K. (2001), *Balancing Act*, Bank Systems and Technology 38, Pp. 22–25

Habib M. and Chen Y. M. (2009), Currency options trading practices and the construction and governance of operational risk: A case study, *Accounting, Auditing & Accountability Journal*, 22:4 Pp. 626–660

Herbert A. S. (1955), A Behavioral Model of Rational Choice, *The Quarterly Journal of Economics,* 69:1 Pp. 99–118

Hoffman D. G. (1998), *New Trends in Operational Risk Measurement and Management*, Operational Risk and Financial Institutions. London: Risk Books, Pp. 29–44

Herring R.J. (2002), The Basel 2 Approach to Bank Operational Risk: Regulation on the Wrong Track, *Journal of Risk Finance,* 4:1 Pp. 42–45

Hussain A. (2000), *Managing Operational Risk in financial Markets*, Oxford: Butterworth-Heinemann

Kaiser, T. and Kohne M. (2006), *An Introduction to Operational Risk*, London: Risk Books

Lewis C. M. and Lantsman Y. (2005), *What is a Fair Price to Transfer the Risk of Unauthorized Trading? A Case Study on Operational Risk*, Operational Risk: Practical Approaches to Implementation, London: Risk Books, Pp. 315–356

Marshall C. (2001), *Measuring and Managing Operational Risk in Financial Institutions*, Singapore: John Wiley & Sons

Meyer J. W. and Brian Rowan (1977), Institutionalized Organizations: Formal Structure as Myth and Ceremony, *The American Journal of Sociology,* 83:2 Pp. 340–363

Milligan J. (2004), *Prioritizing Operational Risk*, Banking Strategies 80:67

Moosa I.A. (2007), Operational Risk: A Survey, *Journal of Financial Markets, Institutions and Instruments*, 16:4 Pp. 167–200

Moosa I.A. (2007a), Misconceptions about Operational Risk, *Journal of Operational Risk*, Pp. 97–104

Muzzy L. (2003), The Pitfalls of Gathering Operational Risk Data, *Risk Management Association Journal,* 85 Pp. 58–62

Nocco B. W. and Stulz R. M. (2006), Enterprise Risk Management: Theory and Practice, *Journal of Applied Corporate Finance,* 18 Pp. 8–20

Power M. (2004), *The Risk Management of Everything: Rethinking the Politics of Uncertainty*, London: Demos

Power M. (2007), *Organized Uncertainty: Designing a World of Risk Management*, Oxford: University Press

Rao, V. and A. Dev, (2006), *Operational Risk: Some Issues in Basel II AMA Implementation in US Financial Institutions in The Advanced Measurement Approach to Operational Risk*, London: Risk Books, Pp. 273–294

Rebonato R. (2007), *The Plight of the Fortune Tellers: Why We Need to Manage Financial Risk Differently*, New Jersey: Princeton University Press

Rosenberg J.V. and Schuermann T. (2006), A general approach to integrated risk management with skewed, fat-tailed risks, *Journal of Financial Economics*, 79 Pp. 569–614

Smircich L. (1983), Concepts of Culture and Organizational Analysis, *Administrative Science Quarterly*, 28 Pp. 339–358.

Stake R. E. (1995), *The Art of Case Study Research*, Thousand Oaks: Sage

Tellis W. (1997), Application of a case study methodology, *The Qualitative Report [On-line serial]*, 3:3

Wei R. (2006), *An Empirical Investigation of Operational Risk in the United States Financial Sectors*. University of Pennsylvania

Wei R. (2007) Quantification of Operational Losses Using Firm-Specific Information and External Databases, *Journal of Operational Risk*, Pp. 3–34

Yin G. W. (1984), *Case Study Research: Design and Methods*, Beverly Hills: Sage