International Review of Financial Analysis 30 (2013) 298–307

Contents lists available at ScienceDirect

International Review of Financial Analysis

Operational risk escalation: An empirical analysis of UK call centres

Cormac Bryce [a,*], Carly Cheevers [b], Rob Webb [c]

[a] Economics and Finance Department, Centre for Risk, Banking and Financial Services, University of Nottingham, United Kingdom
[b] School of Psychology, University College Dublin, Ireland
[c] Department of Law, Economics, Accounting and Risk, Glasgow Caledonian University, United Kingdom

ARTICLE INFO

Available online 25 May 2013

JEL classification:
C12
D23
D20
D83

Keywords:
Operational risk
Risk escalation
Theory of Planned Behaviour
Risk management

ABSTRACT

The paper investigates operational risk reporting behaviour and policy dissemination in the selling of financial products by a major British insurance company's call centres. The analysis of the predispositions of call centre employees to escalate operational risks within their working environment will be measured using the Theory of Planned Behaviour (TPB). The empirical analysis indicates that the effects of 'Attitude' and 'Perceived Behavioural Control' significantly affected an employee's intention to escalate operational risk events. Furthermore, the education and training provided to employees has enabled them to better report operational risk losses/events due to increased certainty of their operational risk losses/events knowledge. The study provides a foundation for future research examining the measurement of 'people risk', the collection of valid operational risk data and encourages policy makers to work alongside the insurance industry to spread best practice in capturing valid data, especially in the light of Solvency II implementation.

1. Introduction

Prominent operational failures resulting in the restructuring or collapse of financial institutions have had a major impact on the financial services industry. Notable examples such as NatWest, Allied Irish Bank and Societe Generale have given rise to an increasing emphasis on operational risk and external risk reporting from governments, bank regulators, auditors and rating agencies (Dobler, 2008; Helbok & Wagner, 2006; Sundmacher, 2006). This was further exacerbated by the 2008 financial crisis in which operational risk management was deemed to have failed to provide, or adequately obtain, risk disclosures (KPMG, 2008).

As a result, the accuracy and validity of risk disclosure, and operational risk in general, form a key element of the proposed Solvency II legislation alongside traditional elements such as minimum capital requirements, supervisory review, and market discipline (KPMG, 2008). Importantly for financial institutions, such regulation vastly increases the amount of internal data collection required to drive both the reliability and validity of any operational risk models which then affects perceived riskiness. If the information being utilised by financial institutions is flawed at any level of its collection then the authorities will not be witnessing an institutions true risk position. It is therefore imperative that the capture of quality data is a main priority for operational risk managers (Bryce, Webb, & Adams, 2011; Embrechts, Furrer, & Kaufman, 2003).

The holistic nature of operational risk has meant that capturing data is challenging and a common one size fits all approach has remained elusive. However, recently the IOR (2010) has proposed the three lines of defence which provides realistic common guidelines for the governance of operational risk management within financial institutions. If followed, this should increase an institutions ability to capture the correct data.

The first line of defence involves day to day risk management at the operational level. The second line of defence refers to the agreed risk policies, appetite and controls which the first line must follow. It is the execution of these 'second line of defence' policies, processes, procedures and controls which the first line of defence may have difficulty implementing. This was highlighted in a recent paper by Bryce et al. (2011) which considers the case of a call centre manager not being able to make any sense of the operational risk escalation process, which in turn led to ineffective escalation of risk events to the second line of defence. The third line of defence is internal audit.

This paper examines an important part of the first line of defence involving risk event capture or escalation when it first enters a financial institution via employees working in a call centre. For the purposes of this study operational risk escalation can be defined as 'the internal process by which real or potential operational risks are reported in a manner that complies with agreed institutional policy'. The rapid development in the 1990s of call centres as a distribution vehicle for financial services has made them strategically important both

* Corresponding author. Tel.: +44 115 846 6690.
E-mail addresses: cormac.bryce@nottingham.ac.uk (C. Bryce), carly.cheevers@ucdconnect.ie (C. Cheevers), robert.webb@gcu.ac.uk (R. Webb).

1057-5219/$ – see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.irfa.2013.05.002

for internal operations and to distribute their portfolio of products and services (Glucksmann, 2004; Malhotra & Mukherjee, 2004). Such growth and importance has been attributed to technological advances, increases in operational efficiency and substantial cost reductions (Bryce, Webb, & Watson, 2010).

However, despite what may seem rather obvious advantages, call centres have found themselves at the centre of a few recent scandals. This is because it is not uncommon for call centre staff to be the first contact with a potential risk event, for example staff could witness or become suspicious of a fraudulent external insurance claim or become aware of a colleague acting suspiciously or not in line with company policy and procedure. These events, if unchecked or not reported can escalate into potentially large losses, fines and further erosion of reputation and consumer confidence. An obvious recent example is the mis-selling of PPI which since 2005 has attracted much scrutiny not least in the way retail financial services and products are sold and distributed in the sector (PWC, 2007). Significantly, £1.9bn in claims were paid out by financial institutions in 2011 alone indicating that financial institutions may lack a clear handle on call centre operations and risk escalation (FSA, 2012).

This paper therefore focuses upon the behavioural intention of call centre staff within a major British insurance company to escalate risk events when advising and selling financial products. The paper is structured as follows. In Section 2 we discuss the importance of the risk escalation process to the measurement and management of operational risk while acknowledging the psychological constructs of decision making. Section 3 will establish the methodology employed in this primary research. In Section 4 the results will be discussed with Section 5 concluding the paper with limitations and areas for future research.

2. Solvency II, operational risk and the importance of risk escalation

The UK financial services sector accounts for over 8% of the UK's GDP and the UK insurance market, the focus of this paper, is the largest in Europe, contributing £10.4bn in taxes, with 74% of all households in the UK using home contents insurance (ABI, 2011). Key to reducing the probability that the mistakes leading up to the 2008 financial meltdown will not be repeated is to ensure that institutions have increasingly robust risk management disclosure systems. Institutions now widely acknowledge that operational risk is strategically important and exhibits characteristics fundamentally different from other risks. However, given that the term 'operational risk' is relatively new in financial institutions, research in this area – while increasing – remains limited (Jobst, 2007).

Pressure to focus upon operational risk is also being asserted by the needs of the imminent Solvency II legislation on the insurance industry. Solvency II, which has more than an essence of Basel II about it, has three pillars and a likewise focus on levels of capital and operational risk. In slight contrast, Solvency II was developed to protect individual policy holders from insurer bankruptcy and focuses on the assessment of all quantifiable risks (underwriting for life, non-life and health, market risk, counterparty default risk, and operational risk) on both the assets and liabilities side of an insurers balance sheet. Like banks, insurance companies are finding overall compliance difficult and the uptake of any hybrid internal approach to the measurement of operational risk for Solvency II compliance especially challenging. This has been attributed to a lack of credible data (as was the case for Basel II) and a lack of robust management infrastructure within Pillar 2 of the operational risk control/assessment frameworks of insurance companies (Bryce et al., 2011; CEIOPS, 2009). However, insurance companies must begin to address these issues and evolve procedures to capture data to comply with either a chosen quantitative or qualitative approach and this will impact on how insurance companies evolve their operational risk.

Qualitative assessments will have a key role to play within Solvency II which establishes a set of minimum requirements designed to ensure the validity of internal risk assessments as inputs to any capital calculations (see BCBS, 2005a,b; CEIOPS, 2009; Cruz, 2004; Davis, 2006; Frachot, Moudoulaud, & Roncalli, 2003; Hoffman, 2002). Such validity is based around independence of the operational risk function, depth and maturity of the operational risk frameworks implementation, good governance by Senior Executives and Boards, reporting and escalation of operational risk to those governance forums, compliance with the supporting policies and processes and validation by internal and/or external audit (BCBS, 2003, 2005a,b; CEIOPS, 2009). For example article CEIOPS 2009, p. 6 Directive article 44 states:

> 'Insurance and reinsurance undertakings shall have in place an effective risk management system comprising strategies, processes and reporting procedures necessary to identify, measure, monitor, manage and report on a continuous basis the risks, at an individual and at an aggregated level, to which they are or could be exposed, and their interdependencies'

However, overall responsibility falls not only on regulators but on the institutions themselves. Internal risk escalation and reporting systems must now form an important component of overall external risk disclosure. It must underpin the robustness of data, allowing regulators and governments to be confident that what financial institutions are actually reporting reflects what is actually happening inside the institution. This is of particular importance when considering the first line of defence because this is where the majority of risks will emanate. For example, Turner and Pidgeon (1997) argue that operational risk reporting systems can in principle be designed to capture risks as they 'incubate', thus enabling a pro-active management of risks. Further arguing that internal operations and reporting systems should be designed to allow efficient risk escalation and encourage the raising of awareness of any perceived risks to the second line of defence — who should then be equipped with the necessary skills and authority to manage them. In essence, operational risk escalation is hierarchical with, in many circumstances, those having the clearest view being those interfacing directly with the external environment.

This hierarchical process of risk escalation and internal reporting is fundamental to the collection of relevant internal loss data for risk reporting and modelling purposes. Past research by Kingsley, Rolland, Tinney, and Holmes (1998) and Andersen (1998) both report that people are the most important resource to the success of a financial institution and also the major contributor to operational risk and risk escalation. This notion is extended in the seminal work of Wahlstrom (2006) who argues that without an effective and transparent risk escalation process it is extremely difficult for operational risk managers in the second line of defence to measure, assess, control or manage the risks within an institution. Further adding that "operational risk is about employees' judgements" finding that staff competence was one of the key issues in the management of operational risk. McConnell (2008) goes further and considers people to be one of the four main causal factors of operational risk events.

Wahlstrom (2006), Kingsley et al. (1998), Andersen (1998) and McConnell (2008) are therefore all in agreement that people are at the centre of operational risk and that financial institutions have often overlooked the importance of their staff via a lack of clear and competent management and/or staff training and/or poor recruitment procedures and/or poor risk culture. Wahlstrom concludes that by focusing on staff an institution could reduce operational risk significantly, for example respondents in Wahlstrom's (2006) study claimed that:

> "people who work in the banks might want to cover up their own mistakes i.e. not to report certain types of operational risk." (page 509)