J. Account. Public Policy 34 (2015) 441–466

Contents lists available at ScienceDirect

J. Account. Public Policy

journal homepage: www.elsevier.com/locate/jaccpubpol

Why firms implement risk governance – Stepping beyond traditional risk management to enterprise risk management

Sara A. Lundqvist *

School of Economics and Management, Knut Wicksell Centre for Financial Studies, Lund University, Box 7080, 22007 Lund, Sweden

A B S T R A C T

Stakeholders of firms have pushed for enterprise risk management (ERM) as a response to flawed risk management and corporate governance systems (Kirkpatrick, 2009). Previous studies explaining why ERM is implemented have been informative but overly simplified. The basic argument presented in this study is that ERM should be seen as a composition of traditional risk management and risk governance, each with their own determining factors. Implementation of risk governance is the active step beyond traditional risk management to ERM. This study addresses the complexity of ERM by dividing it into its traditional risk management and risk governance components and investigating the determinants of these components separately but simultaneously. Based on a survey of 145 firms, empirical evidence suggests that the level of risk governance in a firm is related to the size of the firm, leverage and dividend payments and the chief executive officer's influence on the board; this may suggest that corporate governance motives, like the need for governance, existing governance and the control a CEO has over governance decisions, determine the decision to take the step toward implementing ERM. This study is a step toward clarifying the existing ad hoc theoretical foundations of ERM and implies that firms are implementing ERM in accordance with stakeholder desires for better governance of the risk management system.

* Tel.: +46 462227815.

E-mail address: sara.lundqvist@fek.lu.se

http://dx.doi.org/10.1016/j.jaccpubpol.2015.05.002

1. Introduction

The recent financial crisis can partially be attributed to failures and weaknesses in corporate governance in firms; specifically, risk management systems failed in many cases due to these corporate governance flaws rather than technical risk estimation models and other traditional risk management techniques (Kirkpatrick, 2009). As a response, regulators, auditors, Boards and risk assessment agencies have pushed for more structured and integrated risk management as a way to increase control of the risk management system. The result is a push from many directions for the implementation of enterprise risk management (ERM).[1] However, it is not clear if firms are implementing ERM on a superficial basis simply to appease stakeholders or if it is a thoughtful attempt to enhance the governance of the risk management system.

In previous research the motives for ERM implementation are based on an ad hoc collection of theories. There is no consistency or agreement regarding the underlying theoretical foundation for ERM. Some focus on the relationship between corporate governance and ERM (Desender, 2011). Others refer to traditional capital market imperfections motivating traditional risk management activities such as hedging and corporate insurance demand (Liebenberg and Hoyt, 2003; Pagach and Warr, 2011) or a mixture of motives for risk management, motives for corporate governance, and practical motives (Beasley et al., 2005; Gordon et al., 2009). Pulling from existing literature, there are however two general overarching theoretical motives that are applied when motivating ERM implementation: motives for traditional risk management activities and motives for corporate governance. When empirically testing for determinants, ERM studies use all-encompassing proxies of ERM like the hiring of a CRO or similar risk management position (Liebenberg and Hoyt, 2003; Pagach and Warr, 2011), a survey response on the firm's level of implementation (Beasley et al., 2005), or an aggregated ERM score made up of a number of dimensions (Desender, 2011; Gordon et al., 2009). While these studies have been an informative first step, they fail to take into account the complex nature of ERM, and the motivations are practical and theoretically unorganized.

The basic argument of this study is that motives for ERM implementation can be better studied by more thoroughly addressing the complexity of ERM; the way to do this is by breaking ERM into its essential parts and identifying determinants of each part. ERM is principally synonymous with integration – taking a portfolio view of firm risks (Bromiley et al., 2015). Holistically managing a variety of risks requires a well governed system. ERM can fundamentally be seen as traditional risk management with the addition of risk governance.[2] A traditional risk management process entails individually or in a silo identifying risk, measuring risk, monitoring, and perhaps reporting on risk but with little formality, structure, or centralization; simple examples being an isolated group of individuals in the finance department hedging currency risk or a factory floor manager tracking incidents of injury on the job.

Risk governance as used in this study refers to the direction and control of the risk management system. Risk governance provides the structure of the risk management system and specifies responsibilities, authority, and accountability in the risk management system as well as the rules and procedures for making decisions in risk management. Risk governance is the marriage of corporate governance and risk management, and it is the identifying component of an enterprise risk management system. Aebi et al. (2012) also define the risk management-related corporate governance mechanisms of ERM as risk governance, and they refer to the hiring of a chief risk officer (CRO) and the line of reporting of that CRO. Risk governance is about encouraging a culture of risk-awareness throughout the firm, having an organizational structure to support the risk management system, and having in place governance mechanisms to oversee the system in a formal manner. ERM is a step beyond traditional risk management where additional efforts are made by the firm to unite the risk management process organizationally across internal systems, processes and people (Culp, 2001). Essentially, firms supplement the traditional risk management process with risk governance to achieve an integrated approach to risk management – ERM.

[1] Also referred to as integrated risk management, holistic risk management, strategic risk management, and consolidated risk management.

[2] Risk governance and holistic organization of risk management are interchangeable concepts.