Management Accounting Research 24 (2013) 100–121

Contents lists available at SciVerse ScienceDirect

Management Accounting Research

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

Enterprise risk management and continuous re-alignment in the pursuit of accountability: A German case

Matthäus Tekathen, Niels Dechow *

EBS Business School, Gustav-Stresemann-Ring 3, 65189 Wiesbaden, Germany

ARTICLE INFO

Keywords:
COSO
Enterprise risk management
Alignment
Accountability

ABSTRACT

COSO defines ERM as a set of activities that lead to organizational alignment and accountability, given structured work with stable, mobile and combinable information objects. This study argues against this representation by offering three insights developed from case research. We observe ERM as a practice that oscillates between IT-based representations and social interpretations, which never "adds-up" but creates circulation and movement instead. Rather than to produce a common understanding of corporate affairs, ERM communalizes the process of identifying risks and chances and promotes a quest for accountability. Thus, ERM does not focus on improving performance or compliance. Nevertheless, by separating subjects and objects in the organizational context, ERM creates space for otherness and heterogeneity. To the extent that these are mobilized as resources, ERM might offer "intelligence" beyond the coherence and homogeneity, which accounting systems represent.

1. Introduction

In recent years, corporate risk management, or the lack thereof, has gained considerable attention (Woods, 2009). Demands for corporate governance have been followed up by new risk management concepts (COSO, 2004). New regulation demands investments in risk management practices. Sarbanes-Oxley 404 regulation, for example, requires firms to work with the COSO framework or equivalent standards, such as COBIT (IIA, 2008). The need for external display of internal organizational coherence is more relevant today than it has ever been before (Bhimani, 2009).

Risk management is currently a discipline of everything and nothing (Power, 2004, 2009). Implementations often fail to bring intended benefits (Beasley et al., 2010), perhaps because enterprise risk management (ERM[1]) depends on a firm's calculative culture (Mikes, 2009) and on the choice whether only to count risk, or make them count (Mikes, 2011). Risk management depends on multi-faceted institutional dynamics (Arena et al., 2010), but may only serve the public with certifiable "quasi-commodities" in an ongoing quest for organizational virtue and legitimacy (Power, 2007) beyond the limits of individual accountability (Messner, 2009). Unsurprisingly, some have called for the development of (an ethic for) intelligent accountability (Roberts, 2009).

Taking inspiration from contemporary debates about corporate auditability, governance, and risk management, this study explores the ways in which risk management and accountability are related and the ways in which one contributes to the development or destruction of the other.

* Corresponding author at: Chair of Management Accounting & Control, EBS Business School, Gustav-Stresemann-Ring 3, 65189 Wiesbaden, Germany. Tel.: +49 611 7102 1222; fax: +49 611 7102 10 1222.
E-mail address: niels.dechow@ebs.edu (N. Dechow).

[1] Further abbreviations used: CRC, Corporate Risk Coordinator; DRB, Divisional Risk Board; DRC, Divisional Risk Coordinator; GRB, Group Risk Board; IRM, Integrated Risk Management; RO, Risk Owner; R2C, Risk-2-Chance.

1044-5005/$ – see front matter
http://dx.doi.org/10.1016/j.mar.2013.04.005

For that purpose, we aim to compare the abstracts of a popular risk management concept (COSO, 2004) with a case-based study of ERM in the context in which it is practiced (Hopwood, 1983; Roberts and Scapens, 1985). We want to explore conceptual and practical ERM representation in comparison to accounting. It is relevant for us understand what ERM constitutes, in particular because it has already been suggested that its future will become increasingly intertwined and inextricably interdependent with management accounting and corporate governance (Bhimani, 2009). Moreover, we have found it interesting that COSO makes explicit and frequent reference to the ways in which ERM depends on the construction of organizational alignment and accountability. Hereby, COSO appears to conceptualize ERM as an accounting system that builds its information hierarchy based on stable, mobile and combinable figures (Robson, 1992). In order to prepare for an intelligent (ethic for) accountability, it would be relevant to know *whether ERM practice unfolds itself as accounting (information systems)*. In order to answer this question, we study the technologies by which ERM is mobilized in a firm and attempt to explore what alignment and accountability mean.

Recent risk management studies suggest that firms motivate ERM by focusing on either compliance or performance (Arena et al., 2010; Mikes, 2009, 2011). We are curious to understand, *if and how performance and compliance objectives become constitutive of managerial logics in use* (Giddens, 1976) *or the "rationalizations of work" somewhere in between rhetoric, practice, concept and action* (Ahrens, 1996, 1997). COSO suggests that it is possible to achieve accountability by aligning the processes and people according to their hierarchical role and functional tasks. In that case, one could think that *ERM would involve very specific combinations of information objects and subjects in practice. However, is that the case?* Our exploration of these three questions is based on case research of a German top-tier corporation in which risk management work is set in the context of recent legislative changes at a national level and motivated by a recent publicized compliance problem.

The paper is structured as follows. Section 2 introduces in further detail COSO's conceptualization of ERM (COSO, 2004). Our aim here is to familiarize the reader with ERM as an abstract system design (Roberts and Scapens, 1985) before introducing our research approach in Section 3 and presenting our case in Section 4. In Section 5, we discuss our findings, comparing the COSO concept with a German case practice. Subsequently, in Section 6, we conclude this study, offer practical implications and derive questions for further research.

2. COSO enterprise risk management

In 2004, COSO[2] launched a concept for ERM. It conceptualizes a three-dimensional model with an intention to integrate and align corporate strategic objectives, organizational structure and managerial reporting and control procedures. In line with "modern management", ERM is represented by its own graphic – a three-dimensional cube.

We have studied this conceptualization to understand how enterprises should manage risks according to professional accountancy associations. We chose to look at COSO ERM, because this concept is often referred to as a benchmark risk management approach. In particular, we were curious to learn how this concept defines risk management, accountability and alignment.

The COSO ERM concept defines risk management using a top-down approach that segments managerial responsibilities according to hierarchical positions. It considers, for example, that "*each manager should be accountable to the next higher level for his or her portion of enterprise risk management, with the CEO ultimately accountable to the board*" (COSO, 2004, p. 86). COSO ERM states that accountability develops from everyone in the organization knowing their responsibilities and contributing to the overall mission, vision and objectives of the firm. In other words, COSO ERM adopts a classical view of organizational management, which appears contemporary mainly by its choice of rhetoric. The emphasis on classical hierarchical control and allocation of responsibility is represented by a terminology that visualizes hierarchy as a system of "cascading responsibilities", which coalesce and contribute to an entity's overall objectives – "*a cascading responsibility exists, where each executive is effectively a CEO for his or her sphere of responsibility*" (COSO, 2004, p. 85).

COSO's ERM suggests that managerial alignment of organizational roles and tasks will ensure accountability. In order to assemble risk management as an enterprise-wide activity, COSO suggests that organizations must develop a code of compliance to measure whether everyone adheres to it and acts in accordance with their individual set of defined roles and responsibilities (COSO, 2004). In addition, COSO (2004) stresses a clear separation of duties, checks and balances. For example, it suggests measuring first the alignment of managerial achievement with a code of conduct and subsequently the contribution of the individual to the firm overall (i.e. the global enterprise as one entity).

COSO ERM promotes the assumption that auditability (Power, 2009) is beneficial to the firm. Risk management work is represented in terms of formalized and disclosure-oriented types of work, which is reminiscent of COSO's (1992) internal auditing approach with its emphasis on the traceability of activities. Although it is repeatedly stressed that all "*actions ... coalesce in the entity's enterprise risk management*" (COSO, 2004, p. 86), what this actually means is less clear. COSO appears to suggest that it is possible to produce accountability by paying careful attention to the alignment of processes and the ways in which they are supported by specific activities and tasks. COSO does not address what alignment work entails, how it unfolds and in relation to which particular agendas and/or objects it

[2] Five major professional associations headquartered in the US organized the Committee of Sponsoring Organizations of the Treadway Commission (COSO) in 1985 as an independent private-sector initiative to study the causal factors that can lead to fraudulent financial reporting. COSO's stated goal is to provide "thought leadership" dealing with three interrelated subjects: ERM, internal control and fraud deterrence.