Accounting, Organizations and Society 35 (2010) 659–675

Contents lists available at ScienceDirect

Accounting, Organizations and Society

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

# The organizational dynamics of Enterprise Risk Management

Marika Arena [1], Michela Arnaboldi [*], Giovanni Azzone [2]

*Politecnico di Milano, Dipartimento di Ingegneria Gestionale, Piazza Leonardo da Vinci, 32, 20133 Milano, Italy*

A B S T R A C T

This paper explores the organizational dynamics of Enterprise Risk Management (ERM). ERM is the main form taken by firms' increasing efforts to organize uncertainty, which 'exploded' in the 1990s. The ERM approach seeks to link risk management with business strategy and objective-setting, entering the domains of control, accountability and decision making. In this work, the organizational variations of ERM are investigated through a longitudinal multiple case study, using data from three companies collected over a 7-year period (from 2002 to 2008). The findings contribute to our understanding of ERM as a practice, revealing its trajectory within the organizations as it encounters pre-existing logics, and as both are shaped by risk rationalities, experts and technologies.



## Introduction

> "We now propose to introduce Enterprise Risk Management (ERM) analysis into the corporate credit ratings process globally as a forward-looking, structured framework to evaluate management as a principal component in determining the overall business profile. [...] ERM provides management with information to optimize earnings – and ultimately the firm's value – while staying in a well-defined risk tolerance. [...] ERM also provides a new and clearer language for transferring information about management's intentions and capabilities, which are critical to credit evaluation" (Standard and Poor's, 2007).

Interest in Enterprise Risk Management (ERM) has grown rapidly during the past 15 years, with regulators, professional associations and even rating firms calling for its adoption. In response to this demand, more and more companies are today embracing ERM, yet its implementation remains poorly integrated, with disparate practices grouped under the same label (Mikes, 2005, 2009; Power, 2007). ERM can be viewed as the culmination of the risk management explosion that started in the 1990s, and is touted as a holistic approach for assessing and evaluating the risks that an organization faces. ERM is most frequently defined with reference to the 2004 Guidance document published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which states:

> "Enterprise Risk Management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of the entity's objectives" (COSO, 2004).

The COSO guidance depicts ERM in managerial and prospective light (Burton, 2008), normatively defining specific elements for its implementation, and advocating that it should benefit decision making and management control. Despite the rational approach proposed, the transition of risk management from a narrow, technical focus (Aseeri & Bagajewicz, 2004; Jaafari, 2001; Kalu, 1999; Verbeeten, 2006) to the strategic sphere has turned ERM into a fluid and poorly defined instrument. ERM can be different things in different organizations, or even within the same organization at different times.

* Corresponding author. Tel.: +39 02 23997328; fax: +39 02 23994083.
*E-mail addresses:* marika.arena@polimi.it (M. Arena), michela.arnaboldi@polimi.it (M. Arnaboldi), giovanni.azzone@polimi.it (G. Azzone).
[1] Tel.: +39 02 23994070; fax: +39 02 23994083.
[2] Tel.: +39 02 23996904; fax: +39 02 23994083.

0361-3682/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.aos.2010.07.003

Mikes (2005, 2009) and Power (2007, 2009) highlight this fluidity, pointing out how ERM can vary in its calculative practices, cultural significance, and level of embeddedness. Power (2009), in particular, notes the danger of ERM lapsing into 'rule-based compliance', and failing to become embedded in managers' decision-making and business processes. This eventuality was already borne out by a 2004 PricewaterhouseCoopers survey, in which CEOs said they viewed ERM as an external accountability device that does not impact on managers' decisions and operations (PricewaterhouseCoopers, 2004).

ERM embeddedness has been further emphasized in the wake of the recent financial crisis (McGinn, 2009; O'Donnell, 2009; Price, 2008), calling for "real ERM" (Zolkos, 2008, p. 6). It has been argued that, for ERM to be effective, companies must "look beyond technology to establish a culture of risk management throughout the organization" (Bruno-Britz, 2009, p. 20), and that ERM must permeate existing practices and the individual behavior of managers in everyday decisions (Standard & Poor, 2008). Despite these recommendations, there are as yet few critical contributions exploring how ERM works in practice, and even fewer addressing how its organizational assembling evolves and contributes to a risk management style (Gephart, Van Maanen, & Oberlechner, 2009; Power, 2009).

The present work contributes to filling this gap in our knowledge of the nature of ERM and its organizational coupling, by exploring how it is translated and alters the behavior and mindset of the actors who, in different capacities, participate in managing uncertainty.[3] These dynamics are examined in detail as a situated practice (Chua, 2007), looking at three companies that have implemented ERM approaches. The field work was conducted over a period of 7 years, from 2002 and 2008, using a case study approach. A total of 41 face-to-face interviews were carried out, with 23 informants.

Drawing on Miller and Rose (1992), we adopted an institutional perspective (Greenwood, Oliver, Suddaby, & Sahlin-Andersson, 2008; Lounsbury, 2008) to analyze the ERM dynamics, which was framed around three elements: risk rationalities, uncertainty experts, and technologies. Risk rationalities denotes the discursive and visual domains that frame how uncertainty is conceptualized into risks, eliciting to varying extents apprehension about the unknown and its impact, and an urgency for control. The second element is that of the corporate roles involved in controlling uncertainty, which include not only the ERM orchestrators, usually given the title of Chief Risk Officer (CRO), but also risk specialists, internal auditors and management accountants, who also increasingly aspire to a greater role in risk management (Fraser & Henry, 2007; IMA, 2006). Entwined with these rationalities and experts is the third element of analysis – namely technologies – which denotes the complex sets of practices, procedures and instruments enacted to accomplish the management and control of risks.

[3] Similarly to Miller, Kurunmaki, and O'Leary (2008), we use the term "uncertainties" to denote the wider range of events that can affect organizations, and the term "risks" to denote those phenomena that are conceptualized and managed as risks within companies.

Although the three case studies described in this paper are not intended to be generalizable, the results do highlight some fundamental aspects of ERM, and its differing organizational trajectories, that may also be relevant to other settings. The observed dynamics reveal a continually evolving mutual interaction between ERM and other pre-existing risk management practices, including elements of management accounting. This fluidity is shaped by the organizational setting, by wider control issues, but also by the roles involved. CROs, management accountants, internal auditors, and risk specialists become translators (Latour, 1987) of the different practices. Through their embedded action, they translate the company's' programmatic ambitions, sometimes seizing opportunities to gain additional power, sometimes struggling to secure organizational recognition, and sometimes paying scant attention to practices perceived as mere formal compliance tasks.

Our analysis is developed in the remainder of this paper, which is organized as follows: "The origins of Enterprise-wide Risk Management", below, describes the origins of ERM, its ambitious and universal message, and the challenge of embedding it within organizations; "ERM organizational dynamics: framing the analysis" then introduces the theoretical framework adopted to cast light on the dynamics of ERM translation; the empirical case studies are illustrated in "The research approach"; and the final sections contain a presentation and discussion of the results, followed by some conclusions.

## The origins of Enterprise-wide Risk Management

Recent years have seen an explosion of interest in risk management (Gephart et al., 2009; Power, 2007; Scapens & Bromwich, 2009), which has moved from peripheral functional areas of the organization to the corporate level. Publications, corporate websites and official reports often contain specific sections devoted to how organizations manage their risks. A wide array of risks are considered, including financial exposure, information system interruptions, fraud, client bankruptcies and regulatory changes.

The rise of risk management, which started in the mid 1990s, can be attributed to a number of factors. One, from a rational-economic perspective, is the change in the competitive environment, with a tendency toward greater turbulence and complexity (Chapman & Ward, 2003; Floricel & Miller, 2001; Giddens, 2003; Miller, 1998; Rahman & Kumaraswamy, 2002; Rasmussen, 1997). This is indeed borne out by the types of risks that organizations themselves take into account, such as the ongoing trend toward business process outsourcing (SAP AG, 2007); more complex forms of public sector contracts (for example Commonwealth of Australia, 2006); the emergence of organized stakeholder groups who may put the spotlight on environmental or social issues (Apple, 2008).

Beck (1992) provides an early analysis of this phenomenon, linking it to wider changes in society such as the increasing individualization of behavior and global interconnectivity of entities, which enables events in one part of the world to rapidly affect other parts of the world. This became apparent to all following a series of major financial

and business scandals that occurred during the 1980s and at the beginning of the 1990s, such as Mirror Group Newspapers, Barings Bank, Polly Peck, Maxwell and Guinness.

These events made the risk society (Beck, 1992) visible at the business level; they starkly demonstrated not only that companies can fail, but also that the concatenated consequences of such failures can affect a huge number of actors and the global market as a whole. The UK provides a good example of how governments and financial control bodies responded to the situation by issuing new codes of practice and regulations such as the Cadbury Code (1992), the Hampel Report (Committee on Corporate Governance, 1998), the Turnbull Report (ICAEW, 1999). These new guidances explicitly linked internal controls to risk management and extended beyond the financial sphere, pressuring companies to embrace a broader range of risks in their analysis. The push for a more holistic approach was further reinforced by a second wave of financial scandals that struck companies in various countries beginning in the year 2000, leading to some 'extreme' consequences such as the Enron collapse. These failures prompted the enactment of the Sarbanes-Oxley Act (2002) in the USA, which in practice only served to exacerbate a "process-obsessed risk management of everything" (Power, 2004).

These regulations had impacts that extended well beyond the borders of the nations in which they were issued, inspiring corporate governance reforms in other countries as well.[4] The common thread in all these reforming initiatives was that they framed risk management as a corporate governance requirement, implying a relation with internal control (see, for instance, Fraser & Henry, 2007; Spira & Page, 2003; Woods, 2009). With its incorporation into internal control, the concept of risk became broader and more systemic in aspiration (Power, 2007; Power, Scheytt, Soin, & Sahlin, 2009).

This emergent, all-encompassing approach was formalized in 2004 by the Committee of Sponsoring Organisations of the Treadway Commission (COSO), which issued a "definitive guidance" for building effective Enterprise Risk Management – ERM (COSO, 2004). COSO (2004) envisions a role for ERM in supporting managers at all levels of decision making and planning, and also provides a precise guide for its design and implementation. ERM is represented as a three-dimensional matrix of eight elements deemed essential for achieving strategic, operational, reporting and compliance goals.

Firstly the *internal environment* (1) determines how risk is perceived and addressed by the organization, defining its approach to risk management. *Objective setting* (2) is the process by which the entity's goals are defined and communicated across the organization. *Event identification* (3) encompasses the recognition of internal and external events (both risks and opportunities). *Risk assessment* (4) is the analysis and evaluation of potential risks, considering their frequency of occurrence and their impact. *Risk response* (5) covers the identification of proper actions for responding to risks, and aligning them with the organization's risk appetite. *Control activities* (6) are the policies and procedures for ensuring that risk responses are effectively carried out. *Information and communication* (7) denotes the mechanisms for ensuring effective communication and flows of information across the organization. Finally, *monitoring* (8) refers to the ongoing management activities for verifying the effectiveness of the processes put in place.

As discussed by Power (2007), this aspirational system portrays ERM in an overly-rational light, taking a simplistic view of organizations. The COSO standard imposes a 'mechanical' and cybernetic form of control that is defined in a top-down manner and abstracted from organizational processes, yet highly legitimized (Power, 2007, pp. 76–82). This dissociation from organizational realities, coupled with its legitimizing connotation, has led the ERM label to be applied to widely differing approaches (Mikes, 2005, 2009; Power, 2007), raising the question of what ERM is and becomes in practice.

Mikes (2009) illustrates this variability with the cases of two financial institutions that have different company-wide paradigms, with "diverging organizational significance" (Mikes, 2009, p. 35): ERM by numbers and Holistic ERM. However, the author focuses on the forms of ERM and their possible developments, without investigating the organizational coupling of ERM with other managerial control processes. The latter issue remains largely unexplored (Gephart et al., 2009; Power, 2009), especially in non-financial companies, leaving open the possibility that firms introduce ERM merely as a compliance device, or as a self-contained internal control activity, but without assimilating it more closely into business processes. In order to better understand these divergences of practices, this paper investigates the organizational dynamics of three companies, and the intertwined dimensions involved in ERM implementation. To clarify what these dimensions are and ground our theoretical perspective, the next section illustrates the conceptual framework used to inform the investigation and the interpretation of data.

## ERM organizational dynamics: framing the analysis

The fluidity of ERM, and the extent to which it is coupled with managerial and control processes, tends to be overlooked by universal hierarchical models (Miller, Kurunmaki, & O'Leary, 2008), which conceptualize ERM in regulatory terms. Such models in fact aspire to introduce a new holistic 'philosophy' for detecting and managing risks, but without considering the specificity of organizations. As it enters the organization, ERM inevitably encounters pre-existing domains, giving rise to variations in practices, potentially ranging from forms of mimicry (DiMaggio & Powell, 1983) to substantive change.

To cast light on this heterogeneity, our research is framed within an institutional perspective. In particular, it takes its cue from recent developments (Greenwood et al., 2008; Lounsbury, 2008) calling for a holistic approach to practice, that pays attention to "the broader cultural frameworks that are created and changed by field-level actors, as well as to the lower-level activities

[4] Looking specifically at the Italian context, the self-regulatory code for Italian listed companies was inspired by the UK legislation.

of organizations and other actors that articulate with those frameworks" (Lounsbury, 2008, p. 356).

Within this perspective, the uses and functional properties of ERM approaches to the framing of risk management are seen as mediated by, and mutually affecting, the institutional environment in which they are implemented. In this view, external forces indeed play a role, however a narrow interpretation of institutional dynamics, and in particular of an isomorphic response, fails to consider intra-organizational actions. Highlighting these internal dynamics necessitates following actors in action (Latour, 1987), but in an institutional light, interpreting their behavior and decisions as "enabled and constrained by the prevailing institutional logics" (Thornton & Ocasio, 2008, p. 103).

Without attempting to outline normative categories, understanding heterogeneity of action nevertheless requires defining elements for capturing organizational patterns (Greenwood & Hinings, 1993). To accomplish this, we draw on Miller and Rose (1992) in articulating the dimensions through which both existing and new systems for controlling uncertainty are conceived and translated (Latour, 1987). To cover broader meaning systems, but also the activities of actors who are embedded in these logics (Lounsbury, 2008), we focus on three elements: risk rationalities, uncertainty experts, and technologies.

The first element, risk rationalities, refers to the "domain for the formulation and justification of idealized schemata for representing reality, analyzing it and rectifying it" (Miller & Rose, 1992, p. 178[5]). Companies' efforts to conceptualize uncertainty into manageable and communicable risks, and to appropriately distribute tasks for dealing with them, represent a 'risk rationality' in this sense. ERM, as envisaged by COSO (2004), aspires to challenge pre-existing ways of conceiving uncertainty, in terms of the models for representing the business, its possible failures, and the resultant impacts on performance. Together with the rise of internal controls, these models have become "almost synonymous with ideals of good management" (Miller, Kurunmaki, & O'Leary, 2008, p. 943), and are seen as providing external assurance of a company's ability to sustain a viable pattern of behavior.

ERM has also taken on a 'moral' character, becoming central to the self-regulatory processes of companies, and to making "the inner life of organizations observable" from the outside (Power, 2007, p. 40). However this external exposure, coupled with the link to internal control, creates scope for ambiguity and discretion in how ERM is problematized: ERM aspires to be of managerial benefit, permeating the manner in which individual managers make day-to-day decisions, but it emanates from the domain of internal control, which tends to emphasize values of regulatory compliance and external accountability. This dichotomy engenders a heterogeneity of meanings, which are initially shaped by formal messages (Widener, 2007), and subsequently by the manner in which practices are translated and operationalized (Latour, 1987).

In this process of translation, the concept of ERM is further reflexively refined as managers assign a certain meaning to practices by acting (or not acting) on them. The managerial thrust of ERM is also challenged by the institutionalized values associated with other organizational sub-systems and processes. The existence of established practices may result in a decoupling (Meyer & Rowan, 1977) of new and aspiring risk rationalities, so that previous practices continue to be seen as the legitimate managerial device by which managers and risks are accountable, while ERM is reduced to an add-on for internal control and compliance to external regulations (Bowling & Rieger, 2005; Bruce, 2005; Martin & Power, 2007).

To unravel how different risk rationalities are entangled with and reflected in practices, we need to follow the actors (Latour, 1987), and in particular those organizational roles involved to different extents in conceptualizing and controlling uncertainty. This is the second element of analysis, here referred to as 'uncertainty experts'. Previous research has developed a typology of risk managers (Mikes, 2009; Power, 2007). First, there are the risk management specialists who deal with specific categories of risks (two common examples are financial risk managers and IT risk managers). Risk specialists are in charge of the traditional silos analysis and they are mainly preoccupied with the correct and reliable quantification of probabilities and impacts.

Second, the rise of ERM and risk management has led to the emergence of a new role, the Chief Risk Officer (CRO) (Aabo, Fraser, & Simkins, 2005; Gates, 2006; Hutter & Power, 2005; Lam, 2003; Liebenberg & Hoyt, 2003). CROs differ from risk management specialists in that they are not necessarily experts in calculating risks, but rather act as advisors who support managers in taking responsibility for risks (Power, 2007).

A third professional group playing a role in the sphere of ERM is that of internal auditors. Seizing the opportunity created by the strategic shift in internal controls, internal auditors have sought to expand their professional jurisdiction (Abbott, 1988), most often by appropriating the risk assessment tasks, but sometimes also the entire risk management process (Fraser & Henry, 2007; Page & Spira, 2004). The fourth and final group is that of management accountants, who have traditionally played a key role in controlling uncertainty through the analysis of variances in performance. Moreover, accountants have in recent times been encouraged by their professional associations (IMA, 2006; Pollara, 2008) to take on an ever more active role in risk management, in an attempt to embed this process within performance management.

The mutual entanglement of these groups of actors, along with their embedded agency in conceptualizing uncertainty, are key elements for understanding the organizational dynamics of ERM on two levels. First, these actors can all be translators of ERM in different organizations, or even in the same organization at different times (Aabo et al., 2005; Mikes, 2008; Walker et al., 2002, 2003). Crucially, the decision to assign responsibility for ERM to internal auditors, to a new figure such as a CRO, or to management accountants will influence the organizational meaning of ERM and its internal trajectory. This

[5] Miller and Rose (1992), addressing the problem of state governmentality, speak of "political rationalities".

impact is likely to be reinforced and performed during its translation into practices by the language, understanding and competences of those actors.

Second, the overlapping of different actors, all charged with managing uncertainty, has implications relating to professional rivalry (see, for instance, Mueller & Carter, 2007; Rittenberg & Covaleski, 2001; Seal & Croft, 1997; Shafer & Gendron, 2005; Suddaby, Cooper, & Greenwood, 2007) and professional development (Miller et al., 2008). On the one hand, there is the possibility that occupational groups will compete for control over information, undermining exchanges of data and favoring decoupling (Meyer & Rowan, 1977). On the other hand, there are opportunities for professional development, in which the hybridization of expertise emerges as a crucial factor (Miller et al., 2008).

Finally, the extent to which ERM becomes embedded or decoupled, and whether hybridization is attained or rivalries arise, are revealed by the third element of analysis: technologies. The term technologies here denotes the complex set of practices, procedures and instruments put in place by organizations to carry out strategies and plans (Miller & Rose, 1992). With specific reference to ERM as an aspiring technology, the analysis first tackles its unity and scope. As noted in the preceding sections, some companies implement ERM as a unified practice that covers all risks with a cross-cutting approach, whereas in others ERM is more of an umbrella (Power, 2007) under which separate risk management practices are carried out by different functional areas.

In addition, material ERM systems vary in their specific risk measures. The evaluation of risks can be done qualitatively or quantitatively, using Likert scales or economic and financial measures, and then reported using a variety of tools such as risk maps, risk scorecards, key risk indicators (Lam, 2006), and risk measures such as VAR and RAROC (Holton, 2003; Sarma, Thomas, & Shah, 2003). Finally ERM technologies articulate different relations between business managers and ERM orchestrators. Notwithstanding the COSO prescription that ERM should be highly interactive, real-world practices are very heterogeneous, with some companies adopting interactive approaches while others favor diagnostic systems (Martin & Power, 2007; Mikes, 2009). In short, styles of ERM are likely to vary, as we shall see.

## The research approach

In this work we adopted a case study approach to analyze the organizational dynamics surrounding the implementation of enterprise-wide risk management (ERM). A field study was carried out over a 7-year period from 2002 to 2008 in three private organizations. Non-financial companies were chosen because less attention has been given to the implementation of ERM in such firms. The three organizations were selected from a sample of companies that claimed to have an enterprise-wide risk management process, identified in a previous extensive study (Arena & Azzone, 2007) in which 16 Italian firms (out of 170) were found to use enterprise-wide risk management approaches; this initial sample was then reduced to 13 companies, in order to focus on non-financial firms. Finally, our three case studies were selected to obtain a heterogeneous sample (Lounsbury, 2008), embracing different industries, company sizes and levels of risk; particular attention was given to the core operational processes, the dynamicity of their competitive environment and their recent business history. For reasons of confidentiality, we have used three pseudonyms (*Cicero*, *Phoedrus* and *Virgilio*) in place of the companies' real names.

The first company, *Cicero*, is an Italian provider of a wide range of telecommunications services, an industry that has seen major changes with the introduction of new technologies and the entry of new competitors into the Italian market. The company was founded by an electronic engineer in 1999 and has expanded rapidly since then, going from 50 to 3000 employees and increasing its turnover from 40 million euros to more than 1000 million euros. The company is currently organized into four central staff departments (finance, human resources, security, and legal affairs) and three business units (consumer, business clients and networks). There are also two corporate units – internal auditing and strategic planning – that report directly to the board of directors. Despite *Cicero's* current size, its management style remains highly centralized, with the CEO maintaining strong control over the divisions and a direct relationship with line managers to reinforce the two leitmotivs of the firm: innovation and continuous growth.

The second company, *Phoedrus*, is part of a large Italian group that operates in the oil and gas industry. *Phoedrus* was formed in 2001 from the demerger of its parent company, and operates in the gas market. Its main activities are in Italy, where the gas industry is regulated by a central government authority, which determines revenues *ex ante* through a tariff system. The historical trend shows a stable situation with sales of close to 2000 million euros and a net invested capital of nearly 9000 million euros. The current organizational structure has been in place since 2001; the company consists of a headquarters, eight local districts which supervise the network, and 66 maintenance centers that ensure the service. The headquarters has just a few organizational levels with four operational divisions (Procurement, Project Control, Operations and Security, Health and Environment), six units reporting to the CEO (General Affairs, Investor Relations, Human Resources, Information Technology (IT) Services, Commercial Development and Management Control Unit), and three further units that report directly to the President (External Relations, Internal Audit and Authorities Relations).

The third company, *Virgilio* is part of a large international group that competes in different fields of the automation and information industry. The group engages in a wide array of business activities, characterized by a high degree of competitiveness and dynamism, and has been reshaped several times during its 150-year history, acquiring and disposing of companies and businesses. The Italian subsidiary was opened at the start of the last century under the wing of its parent company. In 2007 *Virgilio* recorded an overall turnover of nearly 2000 million euros, and had more than 5000 employees. Following a major reorganization in 2003, the company is now composed of

five business units (BU) that operate in different business areas. The BUs are coordinated by the Italian headquarters, which is made up of 12 corporate units centralized during the 2003 reorganization. *Virgilio* has a highly interactive and decentralized management style which places great emphasis on human resources – considered to be the company's key asset. Employees receive intensive training continuously throughout their careers, which also includes rotating people to work in different organizational units and in different subsidiaries across Europe.

Table 1 shows the main descriptive parameters of the three selected organizations.

To gain an in-depth understanding of ERM, a longitudinal case study approach was adopted. This choice is consistent with the need to observe organizational dynamics in detail, and with recent calls for adopting this type of investigation in accounting (Chenhall & Euske, 2007; Chua, 2007; Curtis & Turley, 2007; Robson, Humphrey, Khalifa, & Jones, 2007). Information was gathered from a wide variety of sources: all the reports published by the three companies were analyzed, and newspapers were scanned for statements by the top management and other public coverage of the companies. These documents represented the 'official' face of the companies, and proved particularly useful for capturing the risk rationalities and their changes, arising from both ERM and pre-existing practices.

The prolonged time frame of our involvement with *Cicero*, *Virgilio* and *Phoedrus* allowed us to gain sufficient trust to access, assisted by management, internal documents and archival data not usually made available to the public. This documentation helped elucidate the relevance given to different risk practice, the language used when initially presenting ERM, and the modes of interaction between ERM translators and managers. Access to database and archival content was also crucial for understanding the technologies adopted for ERM and other risk practices.

However the study's primary source of data was face-to-face interviews; we formally interviewed 23 managers, carrying out 41 interviews each lasting an average of 2 h. All the interviews were recorded and transcribed, and each transcript was analyzed separately by each author before jointly discussing the results. The empirical material was not codified, but instead analyzed textually, with each author highlighting emergent themes pertaining to the conceptual elements (risk rationalities, uncertainty experts and technologies) and outlining circular and contingent causalities (Morin, 1999). These themes and patterns were cross-checked and then investigated further through additional interviews to clarify competing interpretations. Table 2 lists the key informants in each of the three organizations.

The initial list of informants was extended as we grew more familiar with the situation in each company. In particular, certain risk specialists were not originally included because they were not officially considered part of the ERM process. All the interviews were carried out at the premises of the studied companies. These repeated visits allowed us to see the organizational setting many times over the course of the 7 years, and at different times of the year. We were also given the opportunity to attend official presentations and to subsequently engage in informal conversation with the participants of these meetings.

## ERM variations in practice

In this section we analyze the results of the three studied cases. The empirical evidence is viewed through the lens of the theoretical framework, and presented in four parts: a short introduction; ERM; other processes dealing with uncertainty and their relation with ERM.

### *Cicero*

The official documents and the comments of the informants highlight that *Cicero*'s strategy is centered on technological innovation, which is described as relying on two key elements: first, the company's network, considered to be its distinctive primary asset; second, the advanced use of Information Technology (IT) in providing services.

#### *Enterprise Risk Management: corporate governance*

Enterprise Risk Management was introduced into *Cicero* in 2005. The decision to implement this process was taken directly by the CEO, who wanted *Cicero* to fully conform to the Italian self-regulatory code (Borsa Italiana, 2006), which strongly recommended that listed companies adopt an integrated risk management system. The risk rationality of ERM was thus framed, from its inception, as part of a wider plan for implementing a 'corporate governance' model. The ERM process was presented to all the line managers, but incorporated into a wider presentation on internal controls entitled "corporate governance, internal control and self assessment of risks". Implementing an effective, externally-recognized internal control system

**Table 1**
Case studies.

| Revenues million euros (2007) | Employees | Industry | Group relation | Holding nationality |
|---|---|---|---|---|
| *Cicero* | | | | |
| Nearly 1000 | 3000 | Telecommunications | Holding | Italian |
| *Virgilio* | | | | |
| Nearly 3500 | 9800 | Automation, information and control | Controlled company | Non Italian |
| *Phoedrus* | | | | |
| Nearly 2000 | 2500 | Utility | Controlled company | Italian |

**Table 2**
Interviews.

| Designation | Wider role in the two processes |
|---|---|
| *Virgilio* | |
| Director of accounting finance and controlling | Responsible for budgeting |
| Opportunity and Risk Manager | Responsible for ERM |
| Performance controller in BU 1 | Consultant on data collection and revision |
| Performance controller in BU 2 | Consultant on data collection and revision |
| Corporate function | Participant in negotiation |
| Business Unit Manager | Participant in negotiation |
| Chief audit executive | Responsible for the monitoring of the risk management process |
| Internal auditor | Participant in monitoring of the risk management process |
| *Cicero* | |
| Director of Management Control | Responsible for budgeting |
| Director of strategic planning | Responsible for strategic planning |
| Chief Risk Officer | Responsible for ERM |
| Head of security and IT | Responsible for security and IT risk department |
| Director of IT systems | Responsible for risk management related to IT and privacy |
| Director of security | Responsible for risk management related to business continuity |
| Chief audit executive | Responsible for the monitoring of the risk management process |
| Business Unit Manager | Participant in negotiation |
| Central staff | Participant in negotiation |
| Central staff | Participant in negotiation |
| *Phoedrus* | |
| Director of budgeting and reporting | Responsible for budgeting |
| Chief financial officer | Participant and supervisor of the budgeting |
| Director of Safety, Health and Environment Department | Responsible for risk management (Safety, Health and Environment) |
| Environmental Risk Manager | Responsible for environmental risks |
| Business Unit Manager | Participant in negotiation |
| Corporate function | Participant in negotiation |
| Chief audit executive | Responsible for ERM |

was depicted as crucial to *Cicero* "now that the company is listed on the stock exchange" (informants' words).

In line with this rationality of building a new corporate governance image, responsibility for ERM was assigned to the Internal Auditing Unit (IAU), which was set up in that same year (2005). To assure the requisite competencies, the company hired, as an expert, a former external auditing consultant to take charge of implementing ERM (the Chief Risk Officer). Drawing on his background, and responding to the perceived need to provide external assurances of *Cicero's* reliability, the CRO rigorously adhered to the hierarchical COSO (2004) framework in building the ERM technology.

Together with the internal auditor, the CRO shaped and timed the technology to follow the calendar of internal audit activities. Risk identification formally starts from the objectives defined in the annual plan; managers are asked to define what risks could prevent the company from attaining those goals. The identified risks are then evaluated qualitatively, to define their probability and impact on a three-level scale (high, medium and low). Data is collected comprehensively across the organization, with the involvement of the directors of the central staff departments, the two BU heads and their direct subordinates (second line managers). The resultant analysis of risks is shared with the managers, after which control of the risks is assigned to the actors involved in the mapping. Finally, the internal auditors monitor and review the effectiveness of the entire system. The formal output of the ERM process is a report drafted quarterly for the Executive Committee, and annually for the board of directors.

The formal ERM procedure calls for a high degree of interaction between the CRO and managers; however the interviews revealed that this does not happen in practice. After the first year of implementation the meetings and workshops were not repeated, and the only interaction between the CRO and managers since then has been through the annual questionnaire and the final report sent to them. This rule-based approach shaped and enforced the 'corporate governance' rationality, and created a distance between ERM, the managers and their decision-making setting:

> "The company is still seen from a distance, though interviews are performed with our managers. The analysis addresses certain types of risks, in particular, those risks typical of a listed company which has adopted the IFRS. Actually, these are the items generally managed by the internal auditing" (division manager).

### *Pre-existing practices and ERM assembling*

In addition to ERM, the company has two pre-existing processes, and experts, whose function it is to control uncertainty: Information Technology (IT) risk management, and Operational Planning.

Assessment of IT risks is handled by the Security Department (SD), and its risk rationality is firmly centered on the assets considered most crucial for the businesses' success: the IT network and technology. The SD's risk management is described by the informants as being "a natural part of the operational delivery of services [...]. SD guarantees business continuity, information security

and privacy, reflecting the intention of the founder to ensure better, reliable and differentiated services to customers". This central role of the SD is also evident in *Cicero's* official website, which has a specific section devoted to IT and security risks.

The initial implementation of the IT risks technology was steered by the founder and originally translated by an engineer with expertise in IT services. Currently, the SD is managed by a person with specific training in security management, and previous experience in a large telecommunication company. The SD expert is acknowledged to play a pivotal role in IT risk management: he continually gives technical advice on detecting risks, defines action plans and investments, and monitors the evolution of risk events. All the informants at *Cicero* rely on him to understand the appropriate trade-offs between acceptable risks and investments:

> "Our business is based on IT, on its innovation but also on our ability to provide secure services and business continuity. SD is our reference point in this matter; they understands our needs and we interact with them continuously, finding the best balance between residual risk and investments" (*Business Unit Manager*).

The SD head is the owner of IT risks, and enforces this role by grounding the technology in a recognized standard model for Information Security: ISO 27001. Risk identification is highly granular, and based on a catalogue of nearly 130 questions specifically focused on IT and security matters, such as network access control and malicious software attacks. This list is submitted to the two business units (BU), which evaluate the risks along three dimensions (probability, impact and vulnerability) on a 10-point Likert scale. The questionnaires are then analyzed by the SD, which prepares a plan of action for managing the risks thus identified. During the process, numerous discussions take place between the SD and the managers, to analyze specific issues or risks.

Although the SD team are the reference experts, IT and security risks are detected, monitored and controlled by everyone; this practice is taken for granted: such risks are embedded in the core processes of the company and recognized to be crucial for its survival:

> "You cannot run our business without guaranteeing continuity, security against fraud and so on. If we, all, don't monitor these risk we will lose our clients, our reputation, and hence revenues and profit" (*BU manager*).

The relevance of the SD is further legitimated by its direct relationships with the CEO and the Executive Committee. IT risks are reported to the top management levels on a yearly basis, and the SD head negotiates directly with the Executive Committee on the budget for security costs and investments. This is accomplished through a double negotiation, first with the divisional managers and then with the Executive Committee, aimed at determining the most appropriate trade-offs between investments and residual risk.

It is at this very top level that overall control of uncertainty is accomplished, and that ERM flows into managerial decisions. The SD head is the only informant who acknowledged the value of the risk analysis carried out by the CRO (referred to as "internal audit" by the informant):

> "Regulatory and legal compliance are becoming more and more important for IT and security, and the work done by the internal audit people is precious to us. My colleagues there and I interact very often; they provided us with all the necessary information for keeping up to date with the regulations. When we prepare the plan we also take these types of risks into account." (*SD head*).

In addition to being managed by the SD, risks are also considered in the Operational Planning (OP), governed by the controller. Responsibility for OP has always been assigned to the Management Control Unit (MCU), however the unit has had a turnover of three different managers since 2000. Despite the company's current size, the process remains marked by a small-business mentality. Its steps are not formalized in manuals or procedures, as these are not considered necessary by the controller. The OP technology develops through two main stages. First there is a restricted top-level discussion to define the overall annual targets, during which the MCU plays a marginal role. Then the resulting statements of profit and loss are sent to the BU managers and discussed with them to define the budget forecasts.

After the close of this negotiation, the MCU experts transpose uncertainty into the OP technology. Specifically, the forecasts are integrated with a risk analysis, taking market and regulatory variables into account. A scenario analysis is performed to understand the possible implications of unexpected events on financial performance. A formal report is included in the OP documentation, which presents the results of selected scenarios (usually the worst and best case). These risks are identified and evaluated entirely by the MCU, without any interaction with managers or with ERM experts, even though uncertainties about these areas are also included in ERM evaluations. When we directly asked how their analysis related to ERM/RSA, the answer was:

> "Risk Self Assessment? ERM? What is ERM? Should I know it? [after a direct explanation by the interviewer]. All right, now I remember it is the internal auditing stuff for the executive board. It is indeed crucial to be compliant with these rules now that we are listed on the stock exchange, but their work is totally separate from ours and does not enter into the budgeting" (MCU head).

### *Phoedrus*

Operating activities are the chief preoccupation within *Phoedrus*. The informants emphasized that their overriding priority is to guarantee 'failure-free' operational processes, in line with the principles of a 'high reliability' or 'reliability-seeking' organization (LaPorte & Consolini, 1991). To achieve high reliability, the company has

allocated considerable financial resources to investments in safe technology, choosing this – rather than economic efficiency – as its primary goal.

*Enterprise Risk Management: compliance*

Enterprise Risk Management was introduced into *Phoedrus* in 2003, and was internally labeled *Risk Self Assessment* (RSA). The decision to implement RSA was driven by the parent company, which asked all the subsidiaries to prepare an "ERM-like" risk map, to satisfy the Italian self-regulation code for listed companies (Borsa Italia, 2006). Neither the holding company nor the top management of *Phoedrus* promoted the implementation of ERM. There were no official presentations given to disseminate the initiative, nor was any pressure ever exerted to actually put it into practice.

This lukewarm level of commitment resulted in ERM being implemented as a 'regulatory compliance' practice, with the internal auditor assigned to serve as its lead actor and translator. Due to the lack of urgency surrounding the initiative, the internal auditor struggled to carry out the exercise. RSA was treated by managers as an unavoidable task imposed by the parent company, which did not add value to their existing knowledge:

> "We did not need an instrument for evaluating risks; we know perfectly well where our risks lie. They have not changed since I've been here, and all of us know exactly what our risks are and where to find the information to obtain a picture of the future" (Manager at *Phoedrus*).

The implementation was turned over to the internal auditor with no official presentations or communications. He shaped the technology using the COSO framework as a reference, without any interactions with managers. The only exchanges during the translation were with the internal audit function of the holding company. The internal auditor depicted the technology as enterprise-wide in scope, and implemented it as a questionnaire based on a list of 26 items, embracing different areas: financial, compliance, security, environment and infrastructure. All the line managers were surveyed, and risks were evaluated qualitatively in terms of their probability and impact, using a five-point scale.

Collection of the data proved extremely difficult, and completing the exercise took longer than expected. A summary report was distributed to line managers, but this was only actually used within the internal audit unit for modifying the cycle-audit plan. The risk map has not been updated since 2003, and the RSA exercise was carried out only once. Its only outward visibility is in internal control reports which simply state that "the enterprise-wide risk analysis has been carried out". Though he complained of the difficulty of data collection, the internal auditor also admitted that RSA was a compliance exercise and that he had no desire to enter into managers' decisional centers:

> "The RSA is mainly an exercise; we had to do it, because it was required by the parent company. But we have other tools for managing risks: we use internal standards, we are certified, and there is a unit responsible for environmental and safety risk management" (internal auditor at *Phoedrus*).

*Pre-existing practices and ERM assembling*

*Phoedrus*, like the preceding case, had two pre-existing processes for dealing with uncertainty: the risk analysis for *work, safety and environment* and the *Operational Plan*.

The *work, safety and environment* risk management was introduced in 1994, when *Phoedrus* was still part of its parent company. There were two main pressures for implementing this process: first, a 1994 Italian law requiring companies to conduct a workplace risk analysis and adopt proper measures for safeguarding employees, and secondly the increasing attention given by stakeholders to environmental issues. These external pressures were reinforced by a pre-existing attentiveness to risk within the *Phoedrus* group as a whole, rooted in its core operational processes and the exigency of performing them in a failure-free manner.

However in 1994 a new emphasis was placed on the opportunity of using ERM to enhance relations with external stakeholders. A panel of external experts was asked to formulate guidelines for voluntary environmental reporting, which were soon afterwards implemented across the entire company. The initiative was intensively promoted both internally and externally and, following its demerger from the parent company, *Phoedrus* inherited this sustainability policy. A specific organizational unit was established for managing these risks: the Security, Health and Environment Division (SHED). The person appointed to head the new SHED unit was a chemical engineer who had been working in the group since 1985, and had prior to this been director of an operational gas dispatching plant for 10 years.

The SHED risk technology consists of two separate analyzes: (1) Environmental and (2) Health and Safety. The environmental risk assessment is based on a certified management system, and takes operational activities as its starting point. For each activity, the SHED identifies the risks in normal and emergency conditions, which are then evaluated on a 10-point Likert scale. The risk evaluation is accompanied by a description of the possible consequences to the environment (e.g. temporary disruption for the construction of new transmission infrastructure, or atmospheric emissions from the gas turbines).

The Health and Safety technology instead considers risks within the workplace. In this case there is no formal risk management process, and the SHED performs the analysis directly, examining the various work activities and surveying the opinions and needs of employees. The final report is distributed to the Management Control Unit and to the operational units; the latter then prepare an intervention plan setting out costs and investments for reducing risks, which is discussed and approved annually.

All the informants acknowledged the centrality of these risks to both their operational processes and external image. They also recognized the importance of the SHED experts, who provide valuable advice and assistance for

conforming to standards, obtaining certifications and leading in international rankings. The company's website devotes an entire section to sustainability, in which the role of the SHED is explicitly recognized:

> "Management for sustainable development is based on a Corporate Governance informed by international best practice, the adoption of a Code of Practice, the adoption of the policy of sustainable development, risk management, and an organizational structure that encompasses a specific Health, Safety, Environment, Sustainability and Technologies Department, health, safety, environment and quality management systems". (*Phoedrus website*).

Prior to the introduction of ERM, risks were already considered in a second process: the Operational Plan (OP) (i.e. the budgeting). The OP is governed by the head of the Management Control Unit (MCU), the controller. The current OP technology was translated by the present controller, and consists of three main phases. It begins in March, when the parent company communicates its analysis of the relevant macro-economic variables. On receiving this document, the MCU guides an internal discussion with senior management to define targets for a few variables. On the basis of these data, the MCU drafts a short pre-plan, which is distributed to all the managers for negotiating targets. When the overall target is achieved, the budget is consolidated and the managers' incentives fixed.

With respect to the technology, risks are transposed into the OP through two types of analysis. As in *Cicero*, an initial analysis inserts them after the close of the negotiation with managers. Risks are conceptualized as performance variances, and examined through a sensitivity analysis conducted on four variables deemed to have cross-company impact: gas demand, investments, operating efficiency and financial structure. This analysis is formalized in the final document, which includes a best- and a worst-case scenario. According to the controller, the analysis is carried out with a centralized approach because of the limited and clearly defined range of risks to which their regulated business is exposed:

> Risk is related to uncertainty; risk exists when there are possible variations. In our business we have very few sources of uncertainty, because most of our parameters depend on the authority. The only elements which may vary are those that we already include in the budget: gas demand, investments, operating efficiency and financial structure. (*controller at Phoedrus*)

A second analysis is made on risks drafted by SHED experts. Starting from the list submitted to senior management, the MCU head governs the discussion with site managers who are then required to draw up a plan of investments and costs for guaranteeing failure-free operational processes. The SHED head does not participate in the financial evaluation, but does set out the technical aspects that need to be addressed:

> "I'm not interested in the budget, what we do is provide all the technical information that operational managers need to address in order to reduce and control environmental and safety risks. When there is a legal requirement they know that the intervention is mandatory, in other cases they discuss a plan with the people at the MCU, taking into account that we are certified and always under scrutiny on sustainability issues" (*SHED head at Phoedrus*)

This process is conducted in parallel with the OP consolidation, and is the only area of risk that is discussed with operational managers. Although these risks are neither considered as performance variances, nor tied to managers' incentives, they are treated as priority investments. The MCU experts and the technology support managers in drawing up their plans, which are then consolidated and finally discussed with senior management to verify their financial sustainability. The MCU plays a focal role in calculating and translating these risks into financials, advising operational managers and supporting top management in making decisions. Again, this discussion is depicted by informants as non-problematic, since:

> "Everyone in the company knows that the environment and sustainability are primary issues for running the business and maintaining a relationship of trust with the territory" (*controller at Phoedrus*).

ERM plays no part in all the above risk analyzes, and the informants scarcely remembered the exercise, even after we directly explained it.

### *Virgilio*

The recent history of *Virgilio* has been marred by a salient event that undermined its financial performances and its relationship of trust with shareholders and stakeholders: an investigation into alleged illegal payments. *Virgilio* has also faced legal disputes which have created some difficulties in acquiring new contracts and bidding for public tenders. This situation was the main reason for the major reorganization of *Virgilio* undertaken in 2003.

#### *Enterprise Risk Management: pervasive performance*

Enterprise Risk Management was introduced into *Virgilio* in 2000, in response to a request issued by the parent company to all subsidiaries in 1999:

> "[...]. Risk management is a core function of entrepreneurial activities and requires transparency and control of the risks in our businesses and processes. [...]. Current management systems, structures and processes must ensure that there is an appropriate system of risk management and must comply with the requirements of [law references]. Starting in fiscal 1999, this risk management system will be reviewed by our statutory auditors as part of the annual audit process. [...]. As part of the planning and reporting process, the Corporate Executive Committee is to be informed of major risks, especially those which might threaten the existence of the individual Groups or the company. Subsidiaries will proceed analogously" (*Company Circular, 1999*).

This circular was followed by an official presentation, which set the implementation of risk management as a "core project"; however the emphasis was not placed on compliance with legal requirements, but on the role of risk management in creating value for the group, as asserted in the opening slide of the presentation:

> "Risk management may provide essential benefits for the enhancement of the company value" (*Official Group presentation of Risk Management*).

Moreover, the official presentations established a clear link with financials, framing the risk rationality within the realm of performance. This was enforced by the language and images used, as exemplified by the closing question of the presentation, addressed to all managers:

> "How solid (emphasis in original) is your budgeted/forecasted EBIT?" (*Official Group presentation of Risk Management*).

The implementation was presented as mandatory and urgent, backed up by a precise timescale and detailed descriptions of the organizational roles involved. It envisaged the involvement of three separate experts: a risk management coordinator (CRO); the risk specialists in charge of detecting specific risk categories; and the internal auditor, who validates the effectiveness and efficiency of the risk management system.

Virgilio accordingly began implementation immediately in 1999, and the project was completed in 2000. In line with the parent company's rationality, the process was made enterprise-wide in scope, and the risks were translated as variances in financial results, embracing all events that might affect profit. Pre-existing local risk practices were thus brought together under a process, depicted as unified and labeled "Opportunity and Risk Management" (O&RM). The implementation was initially handled by a manager brought in from the parent company, who reported directly to the CFO.

The conceptualization of risks as performance variances was further emphasized after the 2003 reorganization, when O&RM was hierarchically placed under the Accounting, Finance and Controlling Unit (AFCU), a function newly centralized at the corporate level. A young new expert in planning and control was appointed CRO. The CRO, under the jurisdiction of the AFCU head (the controller), reshaped the O&RM technology, defining a two-level system: at the corporate level, a central Risk Office (employing two people) was set up to coordinate the entire process; five *Opportunity and Risk Managers* (this is their organizational title) were assigned to each BU to internally advise and support managers. In addition, within each BU there are risk specialists who deal with specific risk categories related to their business.

Under the control of the CRO, and with the local support of the O&R managers, the technology was structured into the following four phases: event identification, evaluation, handling and monitoring. The process starts when the AFCU defines and communicates the annual targets to the BUs; in this first phase, managers are asked to provide an initial outlook of the major opportunities and risks related to their objectives. To ensure data uniformity, a risk questionnaire is used which has standard categorizations of risk, including business, operations management, financial, Information Technology, purchasing, legal and compliance, and human resources risks.

In the second phase, the opportunities and risks are evaluated in terms of their impact on EBIT. During these first two phases, the local O&R managers advise the BU managers and their risk specialists on consolidating the risk map; at the same time, they examine the operations of the BU, reporting to the corporate level all the information deemed relevant to controlling risks. The third phase is risk handling, which includes all the measures and methods for reducing risk (probability and/or impact); these can range from risk avoidance to its reduction or transfer. Finally, the system is monitored through risk workshops of the O&R management network.

The O&RM process is presented as an ongoing interaction between the corporate level and the BUs, through which risks are identified and "allocated". The technology relies on a holistic information basis collected from the BUs and other corporate risk specialists (e.g. finance). This pervasive interaction helps position risk as a central issue for managers, and further enforces the rationality of ERM inception:

> "The O&RM supports us in identifying all the possible variances. This analysis is an instrument for formalizing something that each of us is supposed to do when making decisions. However, being required to write down and evaluate opportunities and risks, the level of attention is higher" (*BU Manager at Virgilio*).

The CRO and the five O&R managers advise managers and guide them in reflecting on the relation between risks, performance and their possible trade-offs.

Although their role as experts is recognized, the BU managers are aware that ownership and responsibility for their risks remain within their BU. Only cross-company effects and corporate risks are under the direct responsibility of the CRO. The CRO and the O&RM staff support managers during the process, but challenge them to autonomously set the final level of expected risks (impact on EBIT).

### *Pre-existing practices and ERM assembling*

With the introduction of ERM in 1999 all pre-existing local risk practices were brought together under the O&RM. Furthermore, with the 2003 reorganization, a partnership was established between ERM and other practices dealing with risks, the ERM/budgeting interface is noteworthy.

The budgeting process was profoundly changed in the 2003 restructuring. Prior to this, the process was distributed across the BUs with the corporate level playing only a marginal role in consolidating the data. Managers in the BUs saw the corporate role as useless and aimed only at producing a "formal, long and boring document" (informant's words) for the parent company. The new CFO decided to take advantage of the centralization of corporate functions to redesign the budgeting technology. The task was delegated to the AFCU, and more specifically to

its newly hired director (the controller), who was given the explicit brief of improving performance reporting and transparency, and reducing the distance between corporate services and the BUs:

> "When I arrived here I was told that my unit's goal is to support the whole of *Virgilio's* management. A first goal was to eliminate the gap between the BUs and the corporate level, which was seen as 'an inefficient collector and distributor' of costs. My second goal was to give a complete picture of the performances to all the management: BUs, top levels here, but also to the parent company. Before starting here I spent 2 months in the parent company, they took me out to dinner and told me that all I should try to do was give them a holistic, clear and transparent vision of what was happening here" (*Controller at Virgilio*).

This need for transparency and reliability shaped the reconfiguration of the budgeting technology. The controller saw scope for using ERM to re-conceptualize the rationalities behind his analysis, attempting to enlarge the set of risks and draw clear links between them and performance variances:

> "This is my dream: one day I'd like to be able to read back from every actual event and see that our CRO was able to provide me with the data for detecting it. We are rowing in the same direction; we would like to be able to justify any change to the forecasted profit with a risk we had previously identified" (*Controller at Virgilio*).

The reorganization of budgeting was orchestrated by the controller, alongside the ERM reconfiguration described previously, emphasizing the link between risks and performance. The design phase lasted nearly 10 months, and the new process was run for the first time in 2004. A parallel with ERM was also drawn in the approach, which was designed to guarantee continuous interaction and tension across the whole organization. A dedicated team of five people support the controller at the corporate level, and another five *Performance Managers* advise managers within the BUs.

With respect to technology, all ERM information is used by the controller, and the ERM/budgeting partnership begins even before the formal start of the budgeting process. Joining their expertise, the controller, the CFO and the CRO review the most up-to-date risk map, which is used to gain an understanding of the main risks faced by the company and to fill possible gaps – i.e. unforeseen risks. The map is then presented along with a few other forecasts to the parent company, which uses them as a basis for the initial Planning Document. This document sets out the major targets for *Virgilio* (e.g. percentage cost reductions or increases in productivity).

Circulation of the Planning document formally activates the pervasive process within *Virgilio*, which is conducted over a 7-month period, in three overlapping phases: market analysis; revenues and cost budgeting, and key account definition. In the market analysis phase, one of the corporate functions explores the market trends for each business unit and defines the market shares for the various product families. The second phase, focusing on revenues and costs, opens the negotiation between the corporate level and the BUs. On the basis of the forecasted market trends, each BU defines in detail its expected revenues, and the attendant costs and risks. In this phase, the business units are asked to include in the budgeting all those events having a probability greater than 50%, and a financial impact exceeding a threshold *X*, which varies across divisions. The role of the O&R managers and performance managers within the BUs is crucial here: they challenge managers in consolidating the data and in tracking the links between risks, actions and performance:

> "It was not easy to understand how all these data fit together; we manage a huge amount of information and sometimes you lose the sense of the overall picture. But actually being forced to include the risks in the budgeting we realize that some targets are at risk" (*BU manager at Virgilio*).

The inclusion of risks in budgeting changes the information basis used for the negotiation, in which the controller appears to have an advantage over the BUs. The cross-company map of risks and the information provided by the local people within the BUs sometimes reveals that certain risks have been neglected. When such risks might have a significant impact, a corporate reserve is created, to counterbalance possible risks neglected by division managers. This is a "provision" that is not visible to the business units, but is visible to the parent company:

> "Not all the risks neglected by managers, that we see, will be included in the management reserve; usually we account for big events, such as large project failures, which can have a significant impact on the financial results at the company level. [...]. This prevents the entire company from being penalised by this error, since nearly 50% of manager incentives are tied to the overall result of the subsidiary" (Controller).

If such an event occurs, the management reserve is freed up and the corresponding amount allocated to the business unit responsible for the variance.

ERM ideas impact more directly on targets, with the inclusion of profit at risk as a measure for the BU incentives. In addition, this emphasis on risks also has a more subtle influence on managers' mindsets. When a number is entered into the budget they carefully evaluate all the risks related to it, but they also, conversely, revise the risk map accordingly. As intended by the controller, *managers see ERM and budgeting as closely intertwined*. Risks and their impact on the company's value have become elements that are taken for granted in the daily workings of *Virgilio*, with various roles making important contributions. The controller orchestrates the overall AFCU processes; the CRO coordinates ERM, which managers acknowledge to be beneficial; and the risk specialists maintain their role as owners of specific categories of risks.

In parallel with the negotiation, an analysis is carried out at the corporate level, using historical information to prepare the costs of corporate functions. The third phase is the forecasting of key accounts, which are important clients that significantly contribute to the profit of the

BUs. All the information is consolidated in a document updated monthly, called the ''pocket budget''. This is a diary-size document containing many visual indicators and few numbers. During our site visits, we found that many managers keep this report in their pockets, or at least on their desks, and consider it useful for tracking their performance and the variance between actual and forecasted figures.

## Discussion

The preceding section presented the cases of three non-financial companies that adopted distinct types of Enterprise-wide Risk Management (ERM). The cases show how ERM was realized differently across the organizations. This observation reflects the thread common to all three cases, namely the fluid nature of ERM and its ongoing reciprocal interactions with the other, pre-existing, practices for controlling uncertainty. Each of the three organizations claimed to have adopted ERM as a new form of control over risks, but they also had prior practices in place. These included silo approaches to risk such as environmental and IT risk management, as well as budgeting. The result was a mutual entanglement between the new and pre-established practices, all evolving in a continuous process of translation (Latour, 1987).

These distinct translations can be thought of as lying on a continuum between decoupling (Meyer & Rowan, 1977) and embeddedness (McCreevy, 2008), corresponding to varying degrees of ERM assimilation into the practices and individual working behavior of managers. Furthermore, in one case the implementation gave rise to a new manner (Hopwood, 1978) of jointly managing risks and performance, arising from the partnership between ERM and budgetary control.

Using the theoretical framework developed previously, we can suggest some explanations for the observed organizational dynamics of ERM, even though the results are specific to a particular time and setting. We focus in particular on heterogeneity, and how it emerges when ERM encounters other pre-existing risk practices and their respective rationalities, experts and technologies.

### *Risk rationalities*

The three above-mentioned dimensions – rationalities, experts and technologies – all evolve continuously through circular interactions, yet the cases indicate that the heterogeneity is, in particular, indelibly marked by the risk rationality invoked on ERM inception. In *Phoedrus*, ERM was predominantly framed in terms of a 'compliance' rationality, superficially mimicking the global, self-regulating norms of corporate governance. The same influence is apparent in *Cicero*, however there ERM was actually seen as a tool for building a sound external image of 'corporate governance'. In *Virgilio* ERM acquired a 'pervasive performance' connotation, and was presented as an instrument that provides ''essential benefits for enhancing the company value''.

These rationalities became the domains for the conceptualization of risks, differently instilling an urgency to better understand and control future threats. Such heterogeneity was shaped by a different ethical character (Miller, 2009), i.e. an attempt to elicit fear about possible failures and negative events. This ethical character was then rendered 'real' by the conceptualized nature of ERM risks and impacts, and their proximity to, or distance from, managers and core processes. Finally, an urgency to 'critically envision alternative futures' (Power, 2009) was differently shaped by the language and images used to present ERM, which could enforce or weaken its relevance to individuals as organizational decision makers and world citizens.

Under the 'compliance' rationality which prevailed at *Phoedrus,* ERM did not elicit any type of urgency for further knowledge. All managers seemed to already know the sources of risks, which were in their view fully covered and controlled by the two established processes: SHED and budgeting. There was an ethical link with external stakeholders, however this did not originate from ERM but flowed out of the pre-existing SHED process, which was perceived as crucial for operational security, protection of human lives and, consequently, for reputation.

The 'corporate governance' rationality of *Cicero* emphasized the urgency of providing external assurance, and establishing a new external trust relationship. However, this imperative was constructed mainly as an internal audit responsibility. Managers claimed that the risks attached to the core processes, IT network and technology, were already known and sufficiently well governed by SD risk management, leading to a devaluing of ERM analysis.

Finally, in the 'pervasive performance' rationality of *Virgilio*, ERM was promoted as an organizational and individual responsibility. The ethics of ERM rationality were effectively expanded as a 'problematization' of each manager's organizational responsibilities. The parent company created apprehension about controlling risks by expressing them in terms of likely variance in profit (EBIT) and challenged managers to critically envision future risks and opportunities. This sense of urgency was enforced by the company's recent history, and in particular its legal problems. These events added a nuance to the ethical character of ERM and its potential role in regaining trust with stakeholders, but also engendered an awareness that the previous understanding of risks had been incomplete. The necessity for ERM was inscribed in official documents and presentations, and a pervasive tension about the unknown instilled through images and examples of past, unpredicted failures.

### *Uncertainty experts*

The three risk rationalities (compliance, corporate governance and pervasive performance) entailed different structures of intentionality (Ahrens & Chapman, 2007) and programmatic actions (Miller & Rose, 1992), which were then put into effect through, and in their turn influenced by, the involvement of uncertainty experts and their approach in implementing ERM.

The three companies assigned responsibility for ERM to actors with different types of backgrounds and experience. At *Phoedrus*, the exercise was carried out by the internal auditor, without assigning a dedicated figure to the task.

In *Cicero*, a new person with experience in external auditing was hired to become Chief Risk Officer (CRO), and placed under the jurisdiction of the internal auditor. In *Virgilio*, a new organizational role was established in 1999 (the CRO) and subsequently put under the jurisdiction of the controller.

Observation of these actors reveals how the rationalities further diverged through their embedded action (Thornton & Ocasio, 2008). Though the causality between rationalities, experts and technologies is circular and contingent (Morin, 1999), the micro-dynamics of the actors highlight how heterogeneity was accentuated in two ways: through the experts' approaches, and through their constraints in action.

The approaches diverged first of all in terms of interaction, ranging from a rule-based (Power, 2009) to a social learning (Miller, 2009) style. In *Phoedrus*, in line with the compliance meaning, the interaction was limited to one-shot survey. In *Cicero*, the CRO wanted to challenge the company's risk awareness, but the interaction with managers was mediated by a standard questionnaire, a rule-based logic which emphasized the 'corporate governance' connotation of ERM. At *Virgilio*, the controller and the CRO shaped an interactive and pervasive approach which enabled reciprocal learning. The approaches of the three companies also diverged markedly in terms of the apprehension elicited in managers; in *Cicero* and *Phoedrus*, experts did not create any type of anxiety surrounding ERM, while in *Virgilio* the interaction took the form of a continuous and collective challenge to predict risks and performance variances.

The experts' actions were also influenced by the space which they were able to find and create within the organization, in competition with pre-existing control practices and experts. Where the existing silos approaches and management control appeared to be reliable, assimilation of ERM into managerial practices proved more difficult. In *Cicero* and *Phoedrus*, where there was no sense of apprehension, and none was created upon introducing ERM, entering managers' decisional centers proved more difficult, even when the translator, as in the case of *Cicero*, was willing to do so. In *Virgilio*, the recent failures helped the CRO to carve out space for ERM in the control framework, which was then reinforced by the alliance with the controller.

The space available to ERM translators was also influenced by the type of business. CROs are supposed to be general advisors who connect business areas and risks across the company; but if these are governed by existing core processes and risk specialists, the possibility of gaining managerial relevance is slight. The limiting case of this dynamic occurs in high reliability organizations such as *Phoedrus*, where the company's external reputation and survival are closely bound up with failure-free operational processes. Here, risk specialists are seen as the reference persons and owners of the identified risks, and the role of the CRO is marginal. To a lesser extent, a similar dynamic is visible in *Cicero*, with the centrality attributed to IT technology and networks. At *Virgilio*, on the other hand, ERM and the CRO were favored by the diversity of business areas and technologies, which imparted added value to a holistic approach to risks and to the CRO role.

### *Risk technologies*

This interplay of roles and rationalities was played out in the technologies, which were integrated into the organization to differing extents. *Phoedrus* exemplifies the extreme case of decoupling. The pre-existing risk rationalities and technologies were not challenged by the introduction of ERM. The SHED practices remained the core risk management technology, and no impacts were observed in the budgeting risk analysis. *Cicero* exemplifies a slight 'embeddedness' at the top level, via the executives committee. In particular, it is the SD director who pays most attention to ERM risks, and complements his calculative practice with the risk map defined by the CRO. *Virgilio* exemplifies the deepest level of 'embeddedness', giving rise to a new hybrid ERM/budget 'style' (Hopwood, 1978). With the controller playing an orchestrating role, ERM was designed to serve budgeting and therefore influences the information basis, the negotiation, targets and incentives.

Our findings also show how the organizational meaning attributed to ERM differs depending on the technologies that are adopted, which are in turn determined by the experts' embedded process of translation. Although this is a circular causal relationship, there is one aspect of the technologies which particularly accounts for the divergences between cases: risk measurement. In *Phoedrus*, risk measurement was based on a predefined list of risks, which entailed only a quick, painless, box-ticking exercise for managers. In *Cicero,* on the other hand, risks were directly identified by managers and then qualitatively evaluated. The qualitative nature of the measure, coupled with the lack of face-to-face interactions with the CRO, caused it to be regarded as inaccurate and useless, a perception further emphasized by comparison with the 131-item IT questionnaire, where each item is clearly envisioned as a real threat. In *Virgilio*, ERM risks were rendered relevant to all managers by using impact on profit as a measure. Furthermore the exigency of evaluating risks was finally impressed on managers through the link with incentives and the budgeting process. These technical devices helped to shape the ERM rationality, rendering risks pervasive.

## Conclusions

Enterprise-wide Risk Management (ERM) belongs to a new wave of self-regulating approaches that started to appear during the 1990s. Although ERM emerged in the domain of internal controls, it aims to be a managerial philosophy that "provide[s] reasonable assurance regarding the achievement of entity objectives" (COSO, 2004). This paper has explored this managerial ambition, investigating the nature of ERM and the heterogeneity of its organizational dynamics.

The cases were analyzed through a theoretical lens drawn from Miller and Rose (1992), which we framed around three sensitizing concepts: rationalities, experts

and technologies. Drawing also from practice-theory, these three elements were rendered specific to risk management, building a reference framework for representing the cases and constructing more explanatory offerings. This was made possible by "zooming in" and "zooming out" of practice (Nicolini, 2009), using the concepts to represent the practice and then tracing circular and contingent causalities (Morin, 1999). Through this interrogation of practice, we responded to the call for more organizational studies of risk management (Gephart et al., 2009; Power, 2009), but also to the call for a more holistic approach to practice analysis, that pays attention to broader cultural paradigms (Lounsbury, 2008).

With specific reference to the contribution to risk management as an organizational practice, the cases presented show that, in its managerial guise, ERM introduces a new scientific rationality (Beck, 1992), marking a potential rupture in the company's risk history and sensitivity, but its organizational translations diverge as they encounter pre-existing centers of control and practices. This heterogeneity is explained at the highest level by differing risk rationalities and their potential to challenge the conceptualization of uncertainty. A shift in the decisional mindset and context is shown to be dependent on whether risks are represented as 'real' problems for managers, instilling urgency in the form of a new moral vocabulary, and by visualizing impacts in a manner close to their actions and responsibilities.

However it is through the experts' embedded actions and their mutual entanglement that the translations are revealed. Constrained by the organizational space found within control frameworks and decisional centers, the heterogeneity of practice is then reduced or enlarged by the approaches adopted by the experts. Greater social interactions emerged as crucial for transferring cultural values, problematizing ERM and insinuating apprehension in managers. Though we do not claim that higher interactivity leads to better forecasting, it does move ERM from being a black box of risks and solutions, to a process of confrontation potentially able to prepare managers for a Black Swan (Taleb, 2007).

ERM is then rendered a managerial problem only if the rationalities are reflected in operable technologies. Qualitative risk maps are perceived as being of little use and far removed from managers' decisions, contributing to a positioning of ERM as a governance device. In the case where this was overcome, and risks linked to performance, a new style of ERM-budgeting (Hopwood, 1978) emerged. This in itself raises several questions about budgeting-related issues, such as the change in the negotiation, information asymmetry, creation of reserves and, last but not least, the 'risk' of pushing individual appetite and opportunism even further (Power, 2009).

The investigation of the partnership between ERM and performance management is not, however, the only avenue of research opened up by the present work. Our findings provide explanations, although contingent, of ERM organizational dynamics, which deserve further study. Firstly, the centrality of companies' business histories suggests the need to better understand how dramatic rare (Lampel, Shamsie, & Shapira, 2009) events affect the conceptualization of uncertainty and, in consequence, managers' sense of morality and behavior. Certain recent financial and operational failures would provide fertile ground for this kind of research. Secondly, this work raises questions concerning the generalizability of its results, and the extent to which ERM dynamics depend on sector specificities (e.g. high reliability organizations) and the characteristics of individual companies. Another avenue for further development pertains to the important role of social interaction (Miller, 2009) in the pervasive performance style of ERM. This finding suggests a need to better investigate the social network structures and their relationship with risk sensitivity propagation, but also raises questions about the competencies and capabilities that CROs, seen as network brokers (Kadushin, 2002), should have.

More generally, our findings also respond to the call for a theoretically and institutionally grounded study of practices (Lounsbury, 2008; Nicolini, 2009). Following the actors in action (Latour, 1987) and tracing their interconnections, we build upon the Miller and Rose approach (1992), progressing from the identification of key elements to the explanation of organizational dynamics, albeit related to a particular time and place. Risk rationality emerges as the global, background, conceptual element; it is institutionally embedded by mediators, who act as both localizers and globalizers (Nicolini, 2009). They are localizers in that they translate the cultural framework across the organizational networks, rendering broader issues operable (Miller & Rose, 1992). However they are also globalizers in that they contribute to the strengthening or weakening of cultural meanings and values, contingent on the organizational space which they are able to acquire in the decision making center.

Finally, our work provides evidence supporting the importance of a holistic research approach that considers the behavior of people and their interrelations, along with the technological solutions as they occur in historical events and cycles. This suggests that considerable intellectual benefits could accrue from contamination with other disciplines (such as anthropology), with a view to providing a rich, systemic, yet always contingent, explanations of risk management practice.

## Acknowledgments

The authors kindly thank the two anonymous reviewers for their helpful comments on earlier versions of this paper.

## References

Aabo, T., Fraser, J., & Simkins, B. J. (2005). The rise and evolution of the chief risk officer: Enterprise risk management at hydro one. *Journal of Applied Corporate Finance, 17*(3), 62–75.

Abbott, A. (1988). *The system of professions: An essay on the division of expert labor*. Chicago: University of Chicago Press.

Ahrens, T., & Chapman, C. S. (2007). Management accounting as practice. *Accounting Organization and Society, 32*, 1–27.

Apple (2008). *A greener apple*, (by) Jobs, S. <www.apple.com>.

Arena, M., & Azzone, G. (2007). Internal audit departments: Adoption and characteristics in Italian companies. *International Journal of Auditing, 11*(2), 91–114.

Aseeri, A., & Bagajewicz, M. J. (2004). New measures and procedures to manage financial risk with applications to the planning of gas commercialization in Asia. *Computers and Chemical Engineering, 28*(12), 2791–2821.

Beck, U. (1992). *Risk society: Towards a new modernity*. London: Sage.

Borsa Italiana (2006). *Codice di Autodisciplina delle Società Quotate*. <www.borsaitaliana.it>.

Bowling, B. M., & Rieger, L. (2005). Success factors for implementing enterprise risk management. *Bank Accounting and Finance, 18*(3), 21–26.

Bruce, R. (2005). Swift message on risk management. *Accountancy*(April), 22.

Bruno-Britz, M. (2009). The age of ERM. *Bank Systems & Technology, 1*(February), 20.

Burton, E. J. (2008). The audit committee: How should it handle ERM? *The Journal of Corporate Accounting & Finance, 19*(4), 3–5.

Cadbury, A. (1992). *Report of the committee on the financial aspects of corporate governance*. London: Gee.

Chapman, C., & Ward, S. (2003). Constructively simple estimating: A project management example. *Journal of the Operational Research Society, 54*(10), 1050–1058.

Chenhall, R. H., & Euske, K. J. (2007). The role of management control systems in planned organizational change: An analysis of two organizations. *Accounting, Organizations and Society, 32*, 601–637.

Chua, W. F. (2007). Accounting, measuring, reporting and strategizing – Re-using verbs: A review essay. *Accounting, Organizations and Society, 32*(4–5), 487–494.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2004). *Enterprise risk management framework*. New York: American Institute of Certified Public Accountants.

Committee on Corporate Governance (1998). *Final report [Hampel report]*. London: Gee Publishing.

Commonwealth of Australia (2006). Public private partnerships: Risk management. *Financial Management Guidance*, 18.

Curtis, E., & Turley, S. (2007). The business risk audit – A longitudinal case study of an audit engagement. *Accounting, Organizations and Society, 32*, 439–461.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*, 147–160.

Floricel, S., & Miller, R. (2001). Strategizing for anticipated risks and turbulence in large-scale engineering projects. *International Journal of Project Management, 19*, 445–455.

Fraser, I., & Henry, W. (2007). Embedding risk management: Structures and approaches. *Managerial Auditing Journal, 22*(4), 392–409.

Gates, S. (2006). Incorporating strategic risk into enterprise risk management: A survey of current corporate practice. *Journal of Applied Corporate Finance, 18*(4), 81–90.

Gephart, R. P., Van Maanen, J., & Oberlechner, T. (2009). Organizations and risk in late modernity. *Organization Studies, 30*(02&03), 141–155.

Giddens, A. (2003). *Runaway world: How globalization is reshaping our lives*. London: Routledge.

Greenwood, R., & Hinings, C. R. (1993). Understanding strategic change: The contribution of archetypes. *The Academy of Management Journal, 36*(5), 1052–1081.

Greenwood, R., Oliver, C., Suddaby, R., & Sahlin-Andersson, K. (2008). *Handbook of organizational institutionalism*. London: Sage.

Holton, G. A. (2003). *Value-at-risk: Theory and practice*. San Diego, CA: Academic Press.

Hopwood, A. G. (1978). Towards an organisational perspective for the study of accounting and information systems. *Accounting, Organisations and Society*(3), 3–13.

Hutter, B. M., & Power, M. (2005). *Organizational encounters with risk*. Cambridge University.

ICAEW (1999). *Internal control – Guidance for directors on the combined code [Turnbull report]*. London: Institute of Chartered Accountants in England and Wales.

IMA – Institute of Management Accountants (2006). *Enterprise risk management: Frameworks, elements, and integration, statements on management accounting*. <www.imanet.org>.

Jaafari, A. (2001). Management of risks, uncertainties and opportunities on projects: Time for a fundamental shift. *International Journal of Project Management, 19*(2), 89–101.

Kadushin, C. (2002). The motivational foundation of social networks. *Social Networks, 24*(1), 77–91.

Kalu, T. C. U. (1999). Capital budgeting under uncertainty: An extended goal programming approach. *International Journal of Production Economics, 58*, 235–251.

Lam, J. (2003). *Enterprise risk management: From incentives to controls, Hoboken*. New Jersey: Wiley.

Lam, J. (2006). *Emerging best practices in developing key risk indicators and ERM reporting*. James Lam & Associates, Inc..

Lampel, J., Shamsie, J., & Shapira, Z. (2009). Rare events and organizational learning. *Organization Science, 20*(5), 835–845.

LaPorte, T. R., & Consolini, P. M. (1991). Working in practice but not in theory: Theoretical challenges of high-reliability organizations. *Journal of Public Administration Research and Theory, 1*, 19–47.

Latour, B. (1987). *Science in action: How to follow scientists and engineers through society*. Cambridge, MA: Harvard University Press.

Liebenberg, A. P., & Hoyt, R. E. (2003). The determinants of enterprise risk management: Evidence from the appointment of chief risk officers. *Risk Management and Insurance Review, 6*(1), 37–52.

Lounsbury, M. (2008). Institutional rationality and practice variation: New directions in the institutional analysis of practice. *Accounting, Organizations and Society, 33*, 349–361.

Martin, D., & Power, M. (2007). *The end of enterprise risk management*. Aei-brookings Joint Center for Regulatory Studies, August.

McCreevy, C. (2008). *Speech on corporate governance*. Institute Chartered Secretaries and Administrators (ICSA) EU Corporate Governance Summit, October.

McGinn, K. (2009). Walking on eggshells. *Waste Age, 1*(February), 24.

Meyer, J. W., & Rowan, B. (1977). Institutional organizations: Formal structures as myth and ceremony. *American Journal of Sociology, 80*(4), 340–363.

Mikes, A. (2005). Enterprise risk management in action. *Centre for the analysis of risk and regulation (CARR) discussion paper report series no. 35*.

Mikes, A. (2008). Chief risk officers at crunch time: Compliance champions or business partners? *Journal of Risk Management in Financial Institutions, 2*(1), 7–25.

Mikes, A. (2009). Risk management and calculative cultures. *Management Accounting Research, 20*(1), 18–40.

Miller, K. D. (1998). Economic exposure and integrated risk management. *Strategic Management Journal, 19*(5), 497–514.

Miller, K. D. (2009). Organizational risk after modernism. *Organization Studies, 30*(2/3), 157–180.

Miller, P., Kurunmaki, L., & O'Leary, T. (2008). Accounting, hybrids and the management of risk. *Accounting, Organizations and Society, 33*(7–8), 942–967.

Miller, P., & Rose, N. (1992). Political power beyond the state: Problematics of government. *British Journal of Sociology, 43*, 173–205.

Morin, E. (1999). *La Tête bien faite. Repenser la Réforme – Réformer la Pensée*. Paris: Ed. du Seuil.

Mueller, F., & Carter, C. (2007). We are all managers now': Managerialism and professional engineering in UK electricity utilities. *Accounting, Organizations and Society, 32*(1–2), 181–195.

Nicolini, D. (2009). Zooming in and out: Studying practices by switching theoretical lenses and trailing connections. *Organization Studies, 30*(12), 1391–1418.

O'Donnell, A. (2009). Regaining trust. *Insurance & Technology, 1*(January), 28.

Page, M., & Spira, L. F. (2004). *The turnbull report, internal control and risk management: The developing role of internal audit*. Institute of Chartered Accountants: Scotland.

Pollara, J. B. (2008). FGRC: Seize the opportunity. *Strategic Finance*(May), 58–59.

Power, M. (2004). *The risk management of everything*. London: Demos.

Power, M. (2007). *Organized uncertainty designing a world of risk management*. Oxford University Press.

Power, M. (2009). The risk management of nothing. *Accounting, Organizations and Society, 34*(6–7), 849–855.

Power, M., Scheytt, T., Soin, K., & Sahlin, K. (2009). Reputational risk as a logic of organizing in late modernity. *Organization Studies, 30*(2–3), 301–324.

Price, T. (2008). Uncovering unknown risk. *Wall Street & Technology, 1*(December), 36.

PricewaterhouseCoopers (2004). *Managing risk: An assessment of CEO perspectives*. New York: PwC.

Rahman, M., & Kumaraswamy, M. (2002). Joint risk management through transactionally efficient relational contracting. *Construction Management & Economics, 20*(1), 45–54.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science, 27*(2/3), 183–213.

Rittenberg, L., & Covaleski, M. A. (2001). Internalization versus externalization of the internal audit function: An examination of professional and organizational imperatives. *Accounting, Organizations & Society, 26*(7–8), 617–641.

Robson, K., Humphrey, C., Khalifa, R., & Jones, J. (2007). Transforming audit technologies: Business risk audit methodologies and the audit Weld. *Accounting, Organizations and Society, 32*, 409–438.

SAP AG (2007). *Risk factors and risk management*. Annual report 2007. <http://www.sap.com>.

Sarbanes–Oxley Act of 2002. (2002). *Public Law 107–204. 116 Stat. 745*.

Sarma, M., Thomas, S., & Shah, A. (2003). Selection of value-at-risk models. *Journal of Forecasting, 22*(4), 337–358.

Scapens, B., & Bromwich, M. (2009). Editorial: Risk management, corporate governance and management accounting. *Management Accounting Research, 20*(1), 1.

Seal, W. B., & Croft, L. (1997). Professional rivalry and changing management control approaches in UK clearing banks. *Accounting, Auditing and Accountability Journal, 10*, 60–84.

Shafer, W. E., & Gendron, Y. (2005). Analysis of a failed jurisdictional claim. The rhetoric and politics surrounding the AICPA global credential project. *Accounting, Auditing & Accountability Journal, 18*(4), 453–491.

Spira, L. F., & Page, M. (2003). Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing and Accountability Journal, 16*(4), 640–661.

Standard & Poor's (2007). *Request for comment: Enterprise risk management analysis for credit ratings of nonfinancial companies*. <www.standardandpoors.com/ratingsdirect>.

Standard & Poor's (2008). Enterprise risk management for ratings of nonfinancial corporations. *Ratings Direct, 5*(June).

Suddaby, R., Cooper, D. J., & Greenwood, R. (2007). Transnational regulation of professional services: Governance dynamics of field level organizational change. *Accounting, Organizations and Society, 32*(4–5), 333–362.

Taleb, N. N. (2007). *The Black Swan: The impact of the highly improbable*. Random House.

Thornton, P., & Ocasio, W. (2008). Institutional logics. In R. Greenwood, C. Oliver, R. Suddaby, & K. Sahlin-Andersson (Eds.), *Handbook of organizational institutionalism*. London: Sage.

Verbeeten, F. H. M. (2006). Do organizations adopt sophisticated capital budgeting practices to deal with uncertainty in the investment decision? A research note. *Management Accounting Research, 17*(1), 106–120.

Walker, P., Shenkir, W., & Barton, T. (2002). *Enterprise risk management: Pulling it all together*. Altamonte Springs: Institute of Internal Auditors Research Foundation.

Walker, P. L., Shenkir, W. G., & Barton, T. L. (2003). ERM in practice. *Internal Auditor, 60*(4), 51–55.

Widener, S. K. (2007). An empirical analysis of the levers of control framework. *Accounting, Organizations, and Society, 32*(7–8), 757–788.

Woods, M. (2009). A contingency theory perspective on the risk management control system within Birmingham City Council. *Management Accounting Research, 20*(1), 69–81.

Zolkos, R. (2008). Financial crisis shows real need for ERM. *Business Insurance, 6*(October), 6.