Journal of Risk Research

ISSN: 1366-9877 (Print) 1466-4461 (Online) Journal homepage: http://www.tandfonline.com/loi/rjrr20

Is enterprise risk management real?

Marika Arena , Michela Arnaboldi & Giovanni Azzone

To cite this article: Marika Arena , Michela Arnaboldi & Giovanni Azzone (2011) Is enterprise risk management real?, Journal of Risk Research, 14:7, 779-797, DOI: 10.1080/13669877.2011.571775

To link to this article: http://dx.doi.org/10.1080/13669877.2011.571775

Published online: 09 Jun 2011.

Submit your article to this journal

Article views: 976

View related articles

Citing articles: 13 View citing articles

Full Terms & Conditions of access and use can be found at
http://www.tandfonline.com/action/journalInformation?journalCode=rjrr20

Download by: [University College Dublin] **Date:** 17 August 2016, At: 10:20

Journal of Risk Research
Vol. 14, No. 7, August 2011, 779–797

Routledge
Taylor & Francis Group

Is enterprise risk management real?

Marika Arena*, Michela Arnaboldi and Giovanni Azzone

Department of Management, Economics and Industrial Engineering, Politecnico di Milano, Milan, Italy

(*Received 1 February 2010; final version received 1 February 2011*)

Moving from the growing relevance of the enterprise risk management (ERM) concept, this paper provides empirical evidence of ERM in practice. The paper presents ERM actual uses in a panel of nine Italian companies from different industrial fields and legislative settings and analyses the relationship between the uses and the characteristics of the ERM tool implemented in each case. The data analysis highlights the existence of different activities that are supported by the ERM tool and also different types of use (i.e. responsive, discoursive and prospective) corresponding to a different contribution of ERM to managerial action. These uses related to the specific characteristics of the tools generally indicated with the label 'ERM'.

Keywords: enterprise risk management; uses; ERM tool characteristics; multiple case study

Introduction

In the last decade, enterprise risk management (ERM) has been proposed as a new instrument to predict risks and help organisations achieve their goals. It is centred on the idea of risk management as a transversal process that addresses all those events which could prevent the achievement of corporate objectives. This idea has been formalised in 2004 by the Committee of Sponsoring Organizations of the Treadway Commission that defines ERM as '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 risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives' (COSO 2004, 2). COSO (2004) represents ERM as a three-dimensional matrix, the so-called COSO cube, which encompasses eight interrelated components, namely:

(1) *Internal environment*, that determines how risk is viewed and addressed by the organisation, defining its approach to risk management;
(2) *Objectives setting*, that consists in the process by which the entity's goals are defined and communicated across the organisation;
(3) *Event identification*, that encompasses the recognition of internal and external events (both risks and opportunities), which, if they occur, could affect the achievement of the organisation's objectives;

*Corresponding author. Email: marika.arena@polimi.it

ISSN 1366-9877 print/ISSN 1466-4461 online
© 2011 Taylor & Francis
DOI: 10.1080/13669877.2011.571775
http://www.informaworld.com

(4) *Risk assessment*, including the analysis and the evaluation of potential risks, considering their frequency of occurrence and their impact;
(5) *Risk response*, covering the identification of proper actions for responding to risks, aligning them with the organisation's risk appetite;
(6) *Control activities*, that consist in policies and procedures ensuring that risk responses are effectively carried out;
(7) *Information and communication*, encompassing the mechanisms ensuring effective communication and flows of information across the organisation; and
(8) *Monitoring*, that consists in ongoing management activities and separate evaluations directed to verify the effectiveness of the process.

The above components are presented as necessary to ensure the achievement of the entity objectives across different organisational levels.

Since its publication, the general idea promoted by COSO (2004) has been enthusiastically accepted by both companies and regulators. Recent regulatory programmes and corporate governance reforms stressed the relevance of the development of holistic risk management systems as a mechanism to ensure sound corporate governance (Spira and Page 2003; Power 2004; Price 2008). Also, rating agencies introduced ERM analysis into the corporate credit ratings process, considering it a blueprint of good governance (Standard & Poor's 2008). These pressures, and the related, increasing interest from different parties (e.g. shareholders, internal auditors, etc.), have fostered the diffusion of an 'ERM philosophy', and a growing number of companies claim to have adopted this practice (Beasley, Clune, and Hermanson 2005; Woods 2007).

However, apart from the use of the ERM term and the adhesion to some general principles, two large problems remain unresolved. First, ERM still 'means different things to different people' (Lam 2003, 4). On the one hand, the COSO identifies ERM with a clearly specified tool characterised by defined phases, actors and modes of interaction, current practices suggest a rather diversified situation. Mikes (2009), analysing ERM in the financial service industry, has highlighted the existence of systematic variations in ERM practices. The term ERM can be seen as 'an umbrella' (Mikes 2009) under which there are several diverse risk management techniques and arrangements (Power 2007). Second, the usefulness of ERM has actually been debated and often questioned by scholars and practitioners. ERM proponents argue that this approach benefits firms by promoting increased risk management awareness which may be translated into better operational and strategic decision-making (e.g. Miccolis, Hively, and Merkley 2001; Kleffner, Lee, and McGannon 2003; Liebenberg and Hoyt 2003; Stroh 2005). However, some authors are sceptical about the real impact of ERM, and have pointed out companies where ERM is mainly adopted as a compliance exercise (Bruce 2005; Collier, Berry, and Burke 2007) or as an 'after-the-fact inspection' (Bowling and Rieger 2005). Martin and Power (2007) have highlighted how the principle at the basis of ERM, the identification of all the risks facing an organisation, can induce organisations just to create bureaucratic trails to prove the quality of processes, making the production of evidence 'more important than managing real risks' (Baker 2004; Kilner 2004; Fraser and Henry 2007).

In this context, this paper aims at contributing to the current debate on ERM by answering these research questions (RQs):

(1) To what extent is ERM actually used?
(2) Is there any relation between ERM uses and different characteristics of the ERM tool implemented?

To answer these questions, we carried out a multiple case study in nine Italian companies, all of which claimed to have implemented ERM. The selection of cases was intended to include diversified companies, in relation to their type of industry and level of uncertainty, with the aim of capturing diversities concerning risk management. The study endorsed a multiple-source method for data collection; the central empirical basis was derived from interviews, which involved 30 key informants in the organisations analysed.

Conceptual model

The conceptual model adopted in this work encompasses two main elements, which provide a guide in answering our RQs: (1) ERM uses (related to our first RQ), illustrating the uses of ERM as emerged in both academic and practitioner literature; (2) ERM tool, highlighting the elements relevant to capture the heterogeneity of ERM configurations (related to our second RQ). The two elements, and their relevant dimensions, have been analysed in detail as follows.

ERM uses

Although the claim of COSO (2004) appears univocal, ERM have been used to diverse extents by different companies, and even by the same company over time (Mikes 2009; Arena et al. 2010). Based on previous literature, this section highlights three potential purposes for which ERM can be used: (1) decision-making, (2) compliance to corporate governance codes, (3) internal auditing.

Recently, much attention has been given to how risk management systems can assist managers in decision-making (Woods 2007; Mikes 2009). ERM can in fact be implemented to obtain more information about an organisation's risks, which potentially results in more informed management and better decisions (Protiviti 2005; Woods 2007). An IBM practitioners' survey has confirmed this desire, showing that Chief Financial Officers (CFOs) include risk as one of their primary concerns (IBM BCS 2005). In this context, ERM can be integrated with performance measurement systems to monitor the strategic uncertainties of a firm. Some authors argue that this integration may be made in the balanced scorecard of a company, linking risk management practices to strategic performance measurements (Beasley et al. 2006; Calandro and Lane 2006; Woods 2007). Other researchers have focused on the need to exploit synergies between risk management and planning processes, thus opening new opportunities to predict performance variances and motivate managers (White 2004; Beasley et al. 2006; Beasley and Frigo 2007; McWhorter, Matherly, and Frizzell 2007).

The second use of ERM falls into the sphere of corporate governance. As recent regulations have increased the responsibility of the board of directors concerning risk and internal control, many companies have introduced ERM as an internal control mechanism to cope with new regulatory requirements (e.g. Miccolis, Hively, and Merkley 2001; Spira and Page 2003). A PricewaterhouseCoopers (PwC) survey among global CEOs has shown that ERM is considered a priority among more than

one-third of the interviewed members of boards of directors (38%) (PwC 2004) and the decision to implement ERM is, in many cases, influenced by them (Lam 2001).

Finally, the third use of ERM concerns internal auditing. Professional guidelines clarify the relationship between internal auditing and ERM, specifying that they are two distinct and separate concepts (Practice Advisory 2110 – 1; IIA Position Statement, The Institute of Internal Auditors UK and Ireland 2004). According to IIA – i.e. internal auditors' professional body – the core role of internal auditing in ERM is to provide assurance on the effectiveness of ERM activities, to help ensure that key business risks are managed appropriately (IIA, 2009). However, in practice, we find evidence of different uses of ERM outputs by internal auditors. First, they can exploit ERM results for planning IA interventions (Sarens and De Beelde 2006; Arena and Azzone 2007); in this respect risk assessment is a key element for internal auditing since internal auditors have to identify which areas are potentially subject to higher risk exposures and prepare the audit plan accordingly. Second, De La Rosa (2005) claims that there is a need for integration between audit reports and ERM results; the author highlights this use as important for auditors, in evidencing to line managers the weaknesses of internal controls, and hence improving communication between auditors and auditees (Melville 1999; Sawyer 2003).

ERM tool

To understand how different ERM uses are related to different configurations of ERM, it is necessary to define the dimensions upon which the ERM tool can be articulated. Empirical evidence on the characteristics of ERM in practice is still scarce (Woods 2007, 2009; Mikes 2009; Arena et al. 2010); however, these contributions, combined with the comparison with the various ERM definitions (AIRMIC 2002; Meulbroek 2002; Kleffner, Lee, and McGannon 2003; Lam 2003; Liebenberg and Hoyt 2003; COSO 2004; Protiviti 2005; Gates 2006), allow us to highlight three main components: (1) risk management model, (2) risk evaluation method, and (3) process coordination/ownership.

The risk management model

An analysis of the various ERM models' illustrations (AIRMIC 2002; Meulbroek 2002; Kleffner, Lee, and McGannon 2003; Lam 2003; Liebenberg and Hoyt 2003; COSO 2004; Protiviti 2005; Gates 2006) reveals that all of them stress two characteristics which are considered critical to distinguish ERM from traditional approaches to risk management:

(1) *Comprehensiveness*: ERM should cover different risk categories; and
(2) *Integration*: ERM systems should span all lines of business, functional areas and their reciprocal influence.

Comprehensiveness refers to the *range of risks considered*. In the 1950s and 1960s, risk management was primarily focused on risks that could be dealt with through insurance. Over time, the concept of risk management has evolved, gradually broadening its focus to incorporate different types of risks, also leading to the creation of new risk categories, such as operational risks and reputational risks (Power 2004). In such a context, ERM has been proposed, by professional associations and regulatory bodies (ICAEW 1999; COSO 2004), as a tool to control the variety of strategic,

market, credit, operational and financial risks (ICAEW 1999; DeLoach 2000; Hiles and Barnes 2001; Banham 2004; Crouhy and Galai 2006; Olson and Wu 2007). Compared to previous approaches to risk management, ERM looks way beyond the set of traditionally insurable risks, and seeks to address all of a firm's risks within an organised and coherent framework (Meulbroek 2002).

The second characteristic stressed by ERM promoters is integration, which refers to how risks are governed within all levels and functions of an organisation. Traditional risk management is often described as silo based when the risk categories are managed separately: financial risks are managed by the financial department, IT risks are managed by the IT unit, and so on. With this approach, the different types of risks are identified, classified and managed separately in different sub-parts of the organisation, which use their *local* risk classifications. As a result, aggregations of risk and development of an overall risk strategy are usually lacking, since this model assumes that risks in different parts of the organisation do not influence each other (e.g. Miller 1998; Harrington, Niehaus, and Risko 2002). Unlike this segmental approach, ERM is centred on the idea of risk management as a transversal and unifying process (e.g. Cumming and Hirtle 2001; Lam 2003; Meulbroek 2002; COSO 2004; Beasley, Clune, and Hermanson 2005). Not only does ERM consider different risk categories (i.e. comprehensiveness), but it also treats each risk class as part of the firm's overall risk portfolio, which is managed holistically (Liebenberg and Hoyt 2003). Specific types of risk are no longer confined within the border of dedicated functions, but all the units within the organisations, whose activities could have an impact on a certain type of risk, should be involved in its assessment and management.

Risk evaluation method

The second element characterising the ERM tool is the risk evaluation method (i.e. how risk is measured and represented within the organisation). In the 1990s, wide attention was devoted to the issue of risk assessment and measurement, leading to the widespread technical ideal of risk, as being a product of likelihood and impact. The rise of ERM has focused further attention on the issue of risk measurement, signing the development of 'a whole enterprise risk metric' to evaluate risks (Power 2007).

Normally, an entity's risk evaluation method comprises a combination of qualitative and quantitative techniques. Qualitative techniques include tools such as qualitative scales and factor ratings, risk priority numbers (Franceschini and Galetto 2001), and fuzzy approaches (Carr and Tah 2001). These techniques are used where risks cannot be quantified or when sufficient credible data, required for quantitative evaluation, are not practicably available or not cost-effective. Quantitative techniques are believed to be more precise and are used in more complex and sophisticated activities. Various quantitative risk measurements such as Value at Risk (VaR), capital at risk, risk-adjusted return on capital have emerged (e.g. Holton 2003) under the influence of sector regulations (Basel II 2004). An increasing number of non-financial firms are also adopting them, though, recently, these approaches have come under much criticism (Dowd and Blake 2006; Woods, Dowd, and Humphrey 2008).

Process coordination/ownership

The third element is the ownership of the risk management process. Companies embracing a 'silo' approach to risk management usually establish local, separate risk

management units (e.g. Cumming and Hirtle 2001; Liebenberg and Hoyt 2003). These units are responsible for segmental risks, which are managed locally with limited interaction with other parts of the organisation. Instead, ERM entails an integrated process, which engages people and systems across the organisation and therefore requires higher coordination (Liebenberg and Hoyt 2003; Aabo, Fraser, and Simkins 2005; Gates 2006; Fraser and Henry 2007).

Though there is no consensus on the function or actor that is most suited to coordinate an ERM project (e.g. Liebenberg and Hoyt 2003), the ones who take on this role most frequently are the chief risk officers (CROs), internal auditors and management accountants. The figure of the CRO was first introduced in risk-intensive businesses, such as energy companies and financial institutions, sometimes under different titles, such as Principal Risk Officer, or EVP of Risk Management (Lam 1999; Miccolis, Hively, and Merkley 2001). More recently, this figure has increasingly been adopted in non-financial companies to increase the visibility of risk throughout the company (Hanley 2002); to communicate the risk management goals; to coordinate different stages of the process, and to report on its results (Gates 2006).

The second actor, who sometimes takes on the role of ERM coordinator, is the internal auditor (e.g. Fraser and Henry 2007; Spira and Page 2009). As highlighted previously, the core role of internal auditors in ERM should be to provide assurance on the effectiveness of ERM activities (IIA Position Statement 2004, The Institute of Internal Auditors UK and Ireland 2004). However, looking at current practices, internal auditors often provide consulting services to assist the organisation in identifying, evaluating and implementing risk management methodologies and assume the role of facilitator and organiser of ERM (Arena, Arnaboldi, and Azzone 2006; Sarens and De Beelde 2006; Fraser and Henry 2007). Thus, the role of internal audit in ERM actually changes from that of outside observer to influential insider (e.g. Spira and Page 2009).

More recently, management accountant associations (IMA and CIMA) have also started initiatives to drive accountants to increase their role in orchestrating ERM (Pollara 2008). Although at present their involvement still appears marginal (Collier, Berry, and Burke 2007), there are a few cases in which management accountants have become responsible for risk management coordination (Collier, Berry, and Burke 2007).

Research method and setting

The empirical analysis has been based on a multiple case study, involving nine non-financial Italian organisations from different types of industry and different normative contexts. Non-financial companies were chosen because less attention has been given to the implementation of ERM in such firms. The nine organisations were selected out of a sample of companies that claimed to have an ERM process, these organisations had been identified in a previous extensive study (Arena and Azzone 2007) in which 16 Italian firms (out of 170) were found to use ERM; this initial sample was then reduced to 13 companies, in order to focus on non-financial firms. Finally, nine case studies were selected on the basis of the willingness of the firms to grant access to the researchers and to disclose confidential information. Table 1 shows the main descriptive parameters of the selected

Table 1. Case settings.

Case	Industry	Listing	Size	Interviewees
IND1	Food/beverages	Yes	Between 5.000 mln and 10.000 mln euros	CAE, Line Manager, Controller
IND2	Transportation	Yes	More than 10.000 mln euros	CAE, two Line Managers
IND3	Energy	Yes	More than 10.000 mln euros	CAE, Strategic Planner, Line Manager
IND4	Telecom	Yes	Between 500 mln and 1.000 mln euros	CAE, Line Manager, Controller
IND5	Construction	Yes	Between 1.000 mln and 5.000 mln euros	CAE, Project Manager, Line Manager
IND6	Rubber	Yes	Between 100 mln and 500 mln euros	CAE, Line Manager, Administration and Control Manager
IND7	Public transportation	No	Less than 500 mln euros	CAE, Internal Auditor, CFO, Line Manager
IND8	ICT	Yes	Between 1.000 mln and 5.000 mln euros	CAE, Line Manager, CFO, Project Manager
IND9	Gas transportation	Yes	Between 1.000 mln and 5.000 mln euros	CAE, Internal Auditor, CFO, Line Manager

organisations. For reasons of confidentiality, we have used pseudonyms in place of the companies' real names.

The data were collected between 2006 and 2008; multiple sources were used to investigate the solutions actually implemented by the companies. The main source of data was semi-structured interviews from 30 informants. Overall, 11 interviews were performed with actors in charge of risk management coordination and 19 interviews were performed with 'risk management users'. Follow-up issues were raised subsequent to the initial interview where additional details or clarification were needed. Although with flexibility, the interview protocol addressed the following issues. Related to the first RQ (ERM uses), we discussed the use of ERM information within managerial processes, internal auditing activities, compliance to corporate governance requirements. In this respect, the analysis of public and internal documents was essential to triangulate data (Yin 1994; Denzin and Lincoln 2000). Moving to the second RQ, we tackled the description of the categories of risks included in ERM, its relation with other types of risk management and other risks specialists (if present); roles and responsibilities of different actors in relation to ERM; and risk evaluation methods. The relationship between different ERM uses and ERM configurations was not directly addressed during interviews but derived subsequently by the researchers.

Research setting: the characteristics of the ERM tool

This section provides a preliminary description of the ERM tool adopted in different companies, in order to allow a thorough analysis of the ERM uses. Table 2 summarises the main characteristics of ERM, following the three elements illustrated in the previous section (risk management model, evaluation method and process coordination/ownership). Below we present an overview of each element.

Table 2. ERM characteristics in the analysed cases.

	Comprehensiveness	Integration	Overarching practice	Risk evaluation methods	Ownership	CRO reporting
IND1	Partial, focused on: compliance, financial, safety	Low, three independent systems	None	Multiple: qualitative and quantitative	Multiple	Internal audit
IND2	High	Medium, one formal system still coexists with local informal risk analyses	Risk matrix	One qualitative with financial thresholds	Unique (local risk managers)	Internal audit
IND3	High	High	Risk matrix	Multiple: qualitative and quantitative	Multiple	Accounting
IND4	High	Low, four independent systems	None	Multiple: qualitative and quantitative	Multiple	Internal audit
IND5	High	Medium, two independent systems	None	Multiple: qualitative and quantitative	Multiple	Internal audit
IND6	High	Low, several independent systems	Risk matrix	Multiple: qualitative	Multiple	Accounting
IND7	Partial, focused on: operational	Medium, two independent systems	None	Multiple: qualitative and quantitative	Multiple	Internal audit
IND8	High	High	Variation in EBIT	One quantitative: financial	Unique (local risk managers)	Accounting
IND9	High	Low, several independent systems	None	Multiple: qualitative and quantitative	Multiple	Internal audit

The risk management model

The nine analysed companies have different risk management models, which we defined in term of comprehensiveness and integration.

Moving from comprehensiveness, the analysed companies have risk management tools that range from high to low comprehensive systems. In seven companies, the risk management system addresses different categories of risk, spanning from regulatory and strategic events to operational risks linked to the every-day activities (e.g. adequate coverage of transportation costs; timely updating of antivirus software). In two cases (IND1 and IND7), the range of risks considered is less comprehensive and does not cover some categories of events. Risk management in IND1 (a company operating in the food and beverages industry for travellers) focuses on compliance to regulations, balanced management of cash flows, and the safety of clients and staff on their sites. In IND7, risk management focuses on operative risks.

As concern integration, the situation is much more diversified. Integration is high in two companies (IND3 and IND8), where local risk managers have been put within a central risk management unit. All the local risk managers report to a CRO that aggregates the results of the risk assessment process and analyses potential synergies over different organisational areas. Furthermore, the ERM system is integrated in relevant managerial processes (such as budgeting and strategic planning) that rely on ERM analysis as an instrument to deal with uncertainty. Integration is medium in three companies (IND2, IND5 and IND7) that are characterised by the coexistence of two independent risk management systems. In IND5 there is a risk management system at a corporate level, which is mainly focused on strategic, market and compliance risks and a project risk management system at an operational level. The tool that operationally supports the project risk management is a database which is used to collect information about past and forecasted events. Each event is tracked in terms of type of risk that has occurred (e.g. claims/litigation issues, late response, engineering/design error) and financial variations. In IND7, risk management is up to the maintenance unit, which focuses on operational risks. The company is currently trying to put into place a second, more holistic, system to support the internal auditing activities; however, this initiative is still in the design phase. Finally, IND2 is a particular case, since the official risk management system is one, however, relevant managerial process does not base on it to consider risk-related information but uses a parallel risk analysis, developed locally within the function that is responsible for the specific managerial process (e.g. the strategic planning function relies on its own risk analysis). In the end, integration is low in the remaining companies (IND1, IND4, IND6 and IND9), where there are disparate risk management practices to deal with different types of risks. These processes are almost independent, and do not cross-evaluate or integrate risks. In IND4, for instance, there are four parallel risk management processes: the internal auditing unit, which affirms to have a holistic process (named ERM by informants), actually focuses on compliance and financial reporting; the IT unit deals with IT risks; the financial unit deals with financial risks; and the insurance buying function deals with insurance risks. A similar situation can be seen in IND6 and IND9. Here there is a transversal process (again named ERM) that deals with strategic, market and compliance risks. Other risk specialists deal with specific types of risks (IT, insurance, financial), which are never integrated in the so-called holistic model. In IND1, the three sources of monitored risks are managed separately by three different units. The internal audit unit deals with compliance risks. The planning and control unit deals

with cash flow risks, using a tool called cash flow management. The insurance function looks after risks related to safety.

Risk evaluation method

The second dimension analysed is the risk evaluation method. Here, we give particular attention to the number and type of approaches adopted to assess the risks; and the presence of an overarching measure through which all the risks are aggregated (Table 2). Two companies have a unique method to evaluate risks and an overarching measure: IND2 and IND8. IND2 is characterised by a qualitative evaluation of risks and the use of a risk matrix to aggregate the risk portfolio. Managers are asked to assess risks through a questionnaire, in which they are requested to qualitatively estimate the probability and impact of potential events against three-point (high, medium and low) or five-point scales (high, medium-high, medium, medium-low and low). Qualitative evaluations are guided by quantitative thresholds. For instance, the impact of potential events is assessed against predetermined thresholds with respect to profitability, the company's assets, reputation and operational efficiency. A potential event has a low impact when it causes losses below 2% on the operative result, a medium impact when it causes losses below 10% and a high impact when it causes above 10% on the operative result. The evaluations are then aggregated and the analysis is always completed by a graphical representation of the overall exposition to risk through a risk matrix. The other case with a unitary situation is IND8. Here, managers, in conjunction with the main milestones of the planning process, are asked to provide a forecast of the major opportunities and risks and evaluate them in terms of their impact on Earnings Before Interest and Tax (EBIT). All risks are therefore aggregated based on this measure.

An overarching practice is also used in IND3 that builds a risk matrix to provide an overall picture of the company's risks. However, in this case, different methods are used to evaluate risks. Among the different techniques, particular attention is given to VaR and economic capital (EC). VaR is used to estimate the probability of financial portfolio losses based on the statistical analysis of historical trends and volatilities. EC is the amount of capital the company should have to support taken risks in order to ensure its financial adequacy.

Finally, a patchy situation was evidenced in the other six cases where the risk evaluation is carried out using different methods and there is no overarching practice to cross-assess the company's risks. In all these cases, there is a more holistic approach to risk (often called ERM) which is based on a qualitative risk assessment and synthesised in a risk matrix. This synthesis, however, does not include all the risk categories, but it does cover high-level risks, such as strategic, regulatory and compliance risks. All the other categories of risks are measured with various, different practices. For example in IND1, the cash flow management tool relies on the quantitative financial analysis of different cash flow profiles and the evaluation of the financial impact of missing inflows on the company's cash flow. In IND5, project risks are evaluated in terms of the financial variation, called extra cost, related to each event. Each variation can be positive or negative (i.e. a cost or a saving) and is estimated on the basis of both the historical values of similar events that have already occurred and an ad hoc analysis performed by the project controller. In IND4, IT risks are quantitatively evaluated using physical parameters that are specified by international guidance in the field (such as the number of unauthorised accesses or the number of machines without upgraded software).

Process coordination/ownership

This third dimension provides an organisational perspective of the responsibilities for risk processes and their coordination mechanisms. In the analysed companies, two main sources of differentiation have been found: the organisational positioning of the CRO; and the presence of a unitary responsibility and possible coordination mechanisms (Table 2).

The responsibility for risk management is assigned to a single person only in two cases (IND2 and IND8), where there is a unique unit, headed by the CRO, that is responsible for the coordination of all the risk management activities. In IND2, the CRO is the Chief Audit Executive (CAE). He coordinates 10 local compliance officers, decentralised in each business unit. Compliance officers are in charge of helping managers identify and evaluate risks, consolidate the outcomes of the risk assessment and verify that the corrective actions that have been defined to manage risks are actually put in place. In IND8, the CRO sits at the corporate level in a central risk office within the accounting and control function; the CRO is supported by local risk managers who are assigned to each business unit.

In all the other cases, the responsibility for risk management is not unique and there are multiple actors who deal with different risk management processes, without reporting to a head person. In general, the most holistic approach is coordinated by a CRO, but risk specialists are hierarchically independent of the CRO. In IND6 and IND3, the CROs report to the accounting unit. In the other cases (IND1, IND4, IND5, IND7 and IND9), the holistic risk management system is coordinated by the internal audit unit, which is responsible for the data collection and reporting. Different risk specialists, instead, govern other risk management processes. In IND1, an accountant is responsible for cash flow management. In IND4, the head of the IT unit is responsible for IT risk assessment. In IND5, project controllers are responsible for the operational risk management system. In IND7, the head of the maintenance function is also responsible for operational risk management. In IND9, the head of the Safety Health and Environment department is in charge of risk analysis related to safety and the environment.

Findings

This section illustrates our findings. The first section presents the ERM uses, answering our first RQ ‘To what extent is ERM actually used? (i.e. ERM uses)’; the second section provides an answer to our second RQ, ‘Is there any relation between ERM uses and different characteristics of the implemented ERM tool?’.

ERM uses

In this section, we analyse the uses of ERM in the nine cases. First, we highlight the activities for which ERM is used; then, we analyse the type of use of ERM, a source of variation which emerged from the empirical investigation. Table 3 provides an outline of the activities for which ERM is used, articulated accordingly to the purposes illustrated previously: (1) corporate governance, (2) internal auditing, and (3) decision-making.

Looking at corporate governance, we found three main tasks for which ERM is employed:

Table 3. Uses of the risk management systems.

			Decision-making	
	Corporate governance	IA	Holistic process	Local risk management
IND1	Compliance to Italian CG Code and risk reporting to the AC	Definition of IA plan and integration with IA report		Support to operational decision-making
IND2	Compliance to Italian CG Code, compliance with SOX and risk reporting to the AC	Definition of IA plan and integration with IA report	Support to managers decision-making	Support to operational decision-making
IND3	Compliance to Italian CG Code and risk reporting to the AC	Integration of IA reports	Integration with the strategic planning process. Support to operational decision-making	Support to operational decision-making
IND4	Compliance to Italian CG Code and risk reporting to the AC	Definition of IA plan and integration with IA report		Support to operational decision-making
IND5	Compliance to Italian CG Code and risk reporting to the AC	Definition of IA plan and integration with IA report		Support to operational decision-making
IND6	Compliance to Italian CG Code and risk reporting to the AC	Definition of IA plan and integration with IA report		Support to operational decision-making
IND7		Definition of IA plan and integration with IA report		Support to operational decision-making
IND8	Compliance to Italian CG Code and risk reporting to the AC		Integration with the planning process. Support to strategic and operational decision-making	Support to operational decision-making
IND9	Risk reporting to the AC	Integration of IA reports		Support to operational decision-making

- Corporate governance disclosures about the risk management system, as required by Italian corporate governance code. These disclosures (including corporate governance reports, corporate website areas dedicated to corporate governance, etc.) are currently quite standard, and the informants revealed a focus on describing the general characteristics of the risk management system, posing marginal attention on the risks relevant for the investors.
- Reporting relevant risks to the board of directors and the audit committee. Wider heterogeneity emerged here from the practice; these reports vary from a list of the 10 major risks (e.g. IND5 and IND1) to a detailed analysis of the risk management results (e.g. IND4 and IND3).
- Compliance with the Sarbanes Oxley Act (SOX). In IND2, the risk management system is also the main tool used by the company to ensure compliance with the SOX regulation, and therefore to report on selected types of risks (related to financial reporting).

Diversity emerged, also in relation to internal auditing, though with limited variations; specifically, the analysis has highlighted three activities for which internal auditors use ERM in practice:

- Risk maps comparison. In eight cases, the internal auditors use ERM outputs to compare their own risk map against the one produced by managers.
- Integration of the evidence derived from the risk identification and evaluation made by the managers to support the definition of the audit plan. In seven companies, the internal auditors take into consideration the outcome of the risk management process in the planning of future internal auditing activities.
- Incorporation of the outputs of the risk management processes in the internal audit reports. In three companies (IND1, IND9 and IND5), the internal audit reports also integrate the evidence of the ERM process.

Third, the last use is to support decision-making. In this respect, it is necessary to articulate the uses, making a distinction between the set of activities related to the holistic process (labelled ERM) and local risk specialists (that are not always integrated in ERM, as discussed above). The holistic process is used for decision-making in three cases only (IND2, IND3 and IND8). In these companies, ERM supports decisions at both the corporate, strategic level and at the operational level. At the corporate level, ERM is integrated with strategic planning and budgeting (IND3 and IND8). At the operational level, the analysis performed on different risk categories supports those managers who are responsible for specific functions in making decisions related to their areas of responsibility. Managers who deal with certain risks (such as the IT unit, the environmental department, etc.) benefit from the overall analysis and achieve a better understanding of the impact, at a corporate level, of the events related to their areas.

In all the other cases, the holistic practice is not used for decision-making, but, rather, informants pointed out a use of the traditional risk practices carried out by the risk specialists. For instance, in IND1, the cash flow management tool is used by the financial department to support the definition of regional plans. In IND5, the project risk management supports project managers in their daily activities, as well as in the definition of shared policies for the project portfolio (e.g. the development of new competences; supplier choices). In IND4, IT risk management is one of the main inputs and the financial risk management support decisions in this specific area.

After having analysed the activities in which ERM is used, we move to consider *how* ERM is actually used. Based on the empirical material we identified three different types of use of the systems implemented, that have been labelled: (1) *responsive*, (2) *discoursive*, and (3) *prospective*.

The *responsive* use refers to the cases (IND1, IND5 and IND9) in which ERM is only superficially used for external conformance (Meyer and Rowan 1977). The aim of ERM is to provide a picture of the risk exposure of the company, but this picture is not really used by either decision-makers or process owners. ERM outputs are employed simply to show that a risk analysis has been actually performed to conform to external requirements: corporate governance code (IND1 and IND5), or the request of the parent company (IND9). However, ERM has no real impact on the organisation. This use remains limited to the sphere of external reporting, and even when the output is distributed internally (e.g. internal audit reports), it is completely overlooked and it fails in stimulating any debate or reaction among managers on the evidenced risk areas.

The second type of use – *discoursive* – is associated to the development of a better understanding of the risk profile of the organisation and the subsequent initiation of a transversal debate among different organisational units (IND2, IND4, IND6 and IND7). This use is more extensive compared to the previous case, though it still remains centred on knowledge sharing more than on its formal and explicit use in guiding future actions. ERM outputs are employed at least to start a debate across the organisation in relation to relevant risks, and ERM results are discussed by managers at different levels. In evidencing this use informants explained that ERM outputs are commented during workshops and meetings (that are a common practices in all the four companies); and sometimes ERM information are challenged and criticised (IND2 and IND6), but they help raise a transversal debate and reflection on the company risks. Such confrontations contribute to the building of a risk culture within the organisation, creating arenas in which threads and opportunities are discussed outside the local context of managers' own organisational units.

Finally, the third type of ERM use has been labelled *prospective* (IND3 and IND8). In these cases, managers act proactively for planning future actions relying on ERM analysis. The overall risk analysis allows top managers to gain a better insight into the overall risk exposures, and to take into account this information when they plan their actions. The prospective use of ERM is evident in the integration of ERM in relevant managerial processes. In IND8, the output of the risk analysis is used to support the definition of the annual budget, the long-term planning and the investment decisions. In IND3, ERM is used for strategic planning, scenario analysis and investment decisions.

Uses and characteristics: what is the relationship?

Finally, we analyse the relationship between the uses and the characteristics of the risk management tools that have been adopted. Two main results emerged from the analysis:

- The range of supported activities and the prospective use of ERM are deeply associated to the actual level of integration of the system.
- The organisational actors that are responsible for ERM implementation and management play a key role in determining the uses made by others actors.

Integration is a common key characteristic of those cases in which we found both an extensive use of ERM in terms of the range of activities that are supported (IND3 and IND8) and a prospective orientation of ERM users (IND3 and IND8). Integration ensures that ERM is able to cover both function-specific and corporate decisions, though this result is achieved in different manners. In IND8, integration has been achieved due to the centralisation of the risk processes under the hierarchical line of the CRO's unit, which is now seen as the reference for all risk issues. This formal definition of responsibilities became a statement for managers at two levels; first, it made ERM relevant by defining a new function and putting old practices under its umbrella; second, it emphasised a new need to address risks in different ways, moving towards the integrated view suggested by ERM proponents. This integration has been favoured by, and in turn favoured, the establishment of a unique risk metric. Opportunities and risks are evaluated in terms of their impact on EBIT contributing to create a common language for risk representation, and enabling the inclusion of this information in other managerial processes.

In IND3, instead, the integration with ERM has been pursued fostering a higher coordination, but without putting the risk specialists under the hierarchical line of the CRO. In this case ERM supports decision-making for corporate issues and for the top levels, while function-specific support to lower levels is still provided directly by the risk specialists. The integration and coordination is induced by the presence of an overarching risk matrix that provides a synthesis of the major risks at both the corporate and the operational levels. To build this matrix, the CRO and the risk specialists have to share information about risks that could have an impact on the respective domains, to ensure that some relevant events would not be overlooked at one of the two levels (corporate or operational). Furthermore, they also carefully cross-check their analysis to avoid the enactment of overlapping risk responses (resulting in the same risks being dealt with separately and therefore causing redundancies and inefficiencies). The matrix is actually, and daily, used by managers for scenario analyses and investment decisions and this intensive use further enforces the establishment of a 'virtuous cycle', by increasing the effort put by the CRO and the risk specialists in ensuring coordination and information consistency.

On the contrary, when integration is lower, the actual use of ERM becomes more limited. This is clear in IND2 that provides an intermediate case between the first two companies and the remaining ones: here we found an extensive use of ERM in terms of the range of activities that are supported, though there is a focus on knowledge sharing more than a prospective use. IND2 has centralised the risk processes under the internal audit unit; the risk management model adopted covers different risk sources across different functions and business units, however, without either replacing or integrating local risk practices, that still survive and are used for function-specific purposes. ERM is not explicitly and formally used in prospective processes such as strategic planning, budgeting or investing analysis, diminishing its significance at the managerial level. The ERM coordinator presents ERM results through an overall risk matrix, that synthesises the major risk exposures. This representation is used by the ERM coordinator to discuss with managers, potentially creating higher awareness of relevant risks impinging on different business units. This information contributes to create a transversal understanding of the risk profile and, in the end, managers appear to consider this information in their choices at least *informally*.

Moving to analysing the cases of less extensive use of ERM, we find that all these companies have a fragmented ERM, where a new ERM-like system has been

introduced to answer corporate governance requirements without affecting the operational spheres and without integrating the pre-existing practices in any way. Such lack of integration determines a situation by which decision-making continues to be based on the analysis of pre-existing specialists and the ERM outputs are used for showing compliance with corporate governance requirements and for internal auditing purposes.

The second driver of ERM uses is the figure in charge of coordinating the process. The analysis highlighted that the organisational figures that are responsible of ERM implementation and management play a key role, because they contribute to communicate to other managers the 'scope' of the ERM tool. In several cases, in managers' minds, the 'ERM label' tends to be naturally associated to the high-level corporate governance sphere. The recent governance reforms and new laws that have followed the financial scandals have turned risk-based internal control into 'an all-pervasive organisational, legal and regulatory principle', whereby companies lacking such internal controls also fail to legitimate themselves (Power 2004). This circumstance has contributed to assimilating ERM to a corporate governance requirement. In addition, the new focus of internal auditing on risk management, and the promotion of ERM made by the IIA, both internationally and locally, have reinforced the idea that ERM falls in the audit/governance domain. As a result, ERM tends to be looked at as a compliance problem when managed by internal auditors, even when they aim to cover a facilitating role (IND2). On the other hand, in the two cases that provide evidence of a prospective use of ERM, the responsibility of coordinating the process is up to the accountants or the strategic planning function (IND 3 and IND8).

Furthermore, beside the organisational position of the ERM coordinator, the specific approach they adopt to present ERM to other actors is a key issue. This is critical to make managers understand that ERM analysis is valuable or at least is worth to be considered and maybe challenged. In particular, open debate, presentations and workshops are important to build awareness of the risk profile of the organisation. Instead, when the CROs limit their analysis to high-level risks (e.g. compliance risks) and they just collect information as it is processed by the other functions, without attempting to initiate a debate around these results, the use of ERM remains focused on demonstrating compliance with external requirements.

Conclusions

This study has provided empirical evidence of ERM in practice, analysing its different uses in a panel of nine Italian companies. The paper contributes to the literature in two ways. First, it highlights the relevance of developing an ERM tool that integrates the risk specialists operating at different managerial levels. This can be done either formally by establishing a hierarchical reporting line between the ERM owner and the risk specialists, or informally, inducing higher coordination and exchange of information among them. If this effort is lacking, the use of the ERM tool remains limited and the prospective use of risk management is left to the risk specialists. Second, the paper highlights the relevance of the professional figures involved in the development and management of ERM. The implication of this choice is often overlooked and this task is generally left to the actors that demonstrate themselves to be more willing to take on this role (in several cases the internal auditors). However, such choice has relevant consequences because it enforces the idea – already common among managers – that

ERM falls in the high-level corporate governance sphere, in contrast to the potential use of the tool as prospective and managerial.

These results could be of potential benefit to those practitioners who wish to develop ERM systems in their companies, because they highlight how ERM potential uses are influenced by the characteristics of the tool implemented. From an academic perspective, these findings may also open new research areas. The nuance of cases suggests, for example, further investigation that could focus on specific sectors or types of companies; further extensive studies with a survey methodology could be carried out to generalise the highlighted patterns to a wider sample of companies. This leads to a final consideration on the limitations of this study. The data were collected through a case study methodology in a specific space and time; the results may not be considered universally valid although they were theoretically and empirically cross-referenced to achieve trustworthiness (Denzin and Lincoln 2000).

References

Aabo, T., J. Fraser, and B.J. Simkins. 2005. The rise and evolution of the chief risk officer: Enterprise risk management at hydro one. *Journal of Applied Corporate Finance* 17, no. 3: 62–75.

AIRMIC. 2002. *A risk management standard.* London: The Association Insurance and Risk Managers.

Arena, M., M. Arnaboldi, and G. Azzone. 2006. Internal audit in Italian organizations: A multiple case study. *Managerial Auditing Journal* 21, no. 3: 275–92.

Arena, M., M. Arnaboldi, and G. Azzone. 2010. The organizational dynamics of enterprise risk management. *Accounting Organization and Society* 35, no. 7: 659–75.

Arena, M., and G. Azzone. 2007. Internal audit departments: Adoption and characteristics in Italian companies. *International Journal of Auditing* 11, no. 2: 91–114.

Baker, N. 2004. In the frame? *Internal Auditing and Business Risk*, December: 32–6.

Banham, R. 2004. Enterprising views of risk management: Businesses can use ERM to manage a wide variety of risks. *Journal of Accountancy* 197: 65–71.

Basel II. 2004. *International convergence of capital measurement and capital standards: A revised framework.* Basel: Bank for International Settlements.

Beasley, M., A. Chen, K. Nunez, and L. Wright. 2006. Working hand in hand: Balanced scorecard and enterprise risk management. *Strategic Finance*, March: 49–55.

Beasley, M., and M. Frigo. 2007. Strategic risk management: Creating and protecting value. *Strategic Finance*, May: 25–31.

Beasley, M.S., R. Clune, and D.R. Hermanson. 2005. Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy* 24, no. 6: 521–31.

Bowling, B.M., and L. Rieger. 2005. Success factors for implementing enterprise risk management. *Bank Accounting and Finance* 18, no. 3: 21–6.

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

Calandro, J., and S. Lane. 2006. Insights from the balanced scorecard: An introduction to the enterprise risk scorecard. *Measuring Business Excellence* 10, no. 3: 31–40.

Carr, V., and J.H.V. Tah. 2001. A fuzzy approach to construction risk assessment and analysis: Construction project risk management system. *Advances in Engineering Software* 32: 847–57.

Collier, P.M., A.J. Berry, and G.T. Burke. 2007. *Risk and management accounting.* London: CIMA

Committee of Sponsoring Organizations (COSO). 2004. *Enterprise risk management: Integrated framework.* New York: COSO.

Crouhy, D., and R.M. Galai. 2006. *The essentials of risk management.* New York: McGraw-Hill.

Cumming, C.M., and B.J. Hirtle. 2001. The challenges of risk management in diversified financial companies. *FRBNY Economic Policy Review*, March: 1–17.

De La Rosa, S. 2005. ERM-based audit reports. *The Internal Auditor* 62: 73–6.

DeLoach, J.W. 2000. *Enterprise-wide risk management: Strategies for linking risk and opportunity.* London: Financial Times Prentice Hall.
Denzin, N., and Y. Lincoln. 2000. *Handbook of qualitative research.* Thousand Oaks, CA: Sage.
Dowd, K., and D. Blake. 2006. After VaR: The theory, estimation, and insurance applications of quantile-based risk measures. *Journal of Risk and Insurance* 73: 193–229.
Franceschini, F., and M. Galetto. 2001. A new approach for evaluation of risk priorities of failure modes in FMEA. *International Journal of Production Research* 39: 2991–3002.
Fraser, I., and W. Henry. 2007. Embedding risk management: Structures and approaches. *Managerial Auditing Journal* 22, no. 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, no. 4: 81–90.
Hanley, M. 2002. The greater protector. *CFO Europe* 29: 34.
Harrington, S.E., G. Niehaus, and K.J. Risko. 2002. Enterprise risk management: The case of united grain growers. *Journal of Applied Corporate Finance* 14, no. 4: 71–81.
Hiles, A., and P. Barnes. 2001. *The definitive handbook of business continuity management.* Chichester: John Wiley.
Holton, G.A. 2003. *Value-at-risk: Theory and practice.* San Diego, CA: Academic Press.
IBM BCS. 2005. *The Agile CFO.* Somers: IBM Corporation, Business Consulting Services.
ICAEW. 1999. *Internal control: Guidance for directors on the combined code* [Turnbull Report]. London: Institute of Chartered Accountants in England and Wales.
Kilner, J. 2004. Into the woods. *Internal Auditing and Business Risk*, November: 26–7.
Kleffner, A.E., R.B. Lee, and B. McGannon. 2003. The effect of corporate governance on the use of enterprise risk management: Evidence from Canada. *Risk Management and Insurance Review* 6, no. 1: 53–73.
Lam, J. 1999. *Enterprise-wide risk management and the role of the chief risk officer.* www.erisk.com (accessed July 2010).
Lam, J. 2003. *Enterprise risk management: From incentives to controls.* Hoboken, NJ: Wiley.
Liebenberg, A., and R.E. Hoyt. 2003. The determinants of enterprise risk management: Evidence from the appointment of chief risk officers. *Risk Management & Insurance Review* 6, no. 1: 37–52.
Martin, D., and M. Power. 2007. The end of enterprise risk management. Regulation2point0, working paper series, number 454. AEI-Brookings Joint Center for Regulatory Studies.
McWhorter, L.B., M. Matherly, and D.M. Frizzell. 2007. Recent trends in ERM and literature review. *Management Accounting Quarterly* 8, no. 3: 18–21.
Melville, R. 1999. Control self assessment in the 1990s: The UK perspective. *International Journal of Auditing* 3, no. 3: 191–206.
Meulbroek, L.K. 2002. Integrated risk management for the firm: A senior manager's guide. *Journal of Applied Corporate Finance* 14: 56–70.
Meyer, J.W., and B. Rowan. 1977. Institutionalized organizations: Formal structure as myth and ceremony. *The American Journal of Sociology* 83, no. 2: 340–63.
Miccolis, J., K. Hively, and B. Merkley. 2001. *Enterprise risk management: Trends and emerging practices.* Altamonte Springs, FL: Institute of Internal Auditors Research Foundation.
Mikes, A. 2009. Risk management and calculative cultures. *Management Accounting Research* 20, no. 1: 18–40.
Miller, K.D. 1998. Economic exposure and integrated risk management. *Strategic Management Journal* 19, no. 5: 497–514.
Olson, D., and D. Wu 2007. *Enterprise risk management.* Singapore: World Scientific Publishing.
Pollara, J.B. 2008. FGRC: Seize the opportunity. *Strategic Finance*, May: 58–9.
Power, M. 2004. *The risk management of everything.* London: Demos.
Power, M. 2007. *Organized uncertainty: Designing a world of risk management.* Oxford: Oxford University Press.
Price, T. 2008. Uncovering unknown risk. *Wall Street & Technology*, December 1.
PricewaterhouseCoopers (PwC). 2004. *Managing risk: An assessment of CEO perspectives.* New York: PwC.
Protiviti. 2005. *US risk barometer.* New York: Protiviti.
Sarens, G., and I. De Beelde. 2006. Internal auditors' perception about their role in risk management: A comparison between US and Belgian companies. *Managerial Auditing Journal* 21, no. 1: 63–80.

Sawyer, L.B. 2003. *Sawyer's internal auditing: The practice of modern internal auditing.* Altamonte Springs, FL: Institute of Internal Auditors.

Spira, L.F., and M. Page. 2003. Risk management: The reinvention of internal control and the changing role of internal audit. *Accounting, Auditing & Accountability Journal* 16, no. 4: 640–61.

Spira, L.F., and M. Page. 2009. Regulation by disclosure: The case of internal control. *Journal of Management & Governance* early view 14, no. 4: 409–33.

Standard & Poor's. 2008. Enterprise risk management for ratings of nonfinancial corporations. *Ratings Direct,* June 5. www.standardandpoors.com/ratingsdirect (accessed July 2010).

Stroh, P.J. 2005. Enterprise risk management at United Healthcare. *Strategic Finance*, July: 27–35.

The Institute of Internal Auditors (IIA). 2009. *International professional practices framework.* Altamonte Springs, FL: Institute of Internal Auditors.

The Institute of Internal Auditors UK and Ireland. 2004. *The role of internal audit in enterprise-wide risk management.* Position Statement. London: The Institute of Internal Auditors.

White, L. 2004. Management accountants and enterprise risk management. *Strategic Finance* 86, no. 5: 6–7.

Woods, M. 2007. Linking risk management to strategic controls: A case study of Tesco plc. *International Journal of Risk Assessment and Management* 7: 1074–88.

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

Woods, M., K. Dowd, and C. Humphrey. 2008. The value of risk reporting: A critical analysis of value-at-risk disclosures in the banking sector. *International Journal of Financial Services Management* 3: 45–64.

Yin, R.K. 1994. *Case study research: Design and methods.* Thousand Oaks, CA: Sage.