Managerial Auditing Journal

A framework for enterprise risk identification and management: the resource-based view

Birendra K. Mishra, Erik Rolland, Asish Satpathy, Michael Moore,

A framework for enterprise risk identification and management: the resource-based view

Birendra K. Mishra
School of Business, University of California Riverside, Riverside, California, USA

Erik Rolland
College of Business Administration, California State Polytechnic University, Pomona, California, USA

Asish Satpathy
Department of Information Systems, W. P. Carey School of Business, Arizona State University, Tempe, Arizona, USA, and

Michael Moore
College of Business Administration, Loyola Marymount University, Los Angeles, California, USA

Abstract

Purpose – This study aims to examine the factors influencing enterprise risk management and propose a framework for identifying and explaining the components of enterprise risk management. To enable broader analytical thinking about risk factors, the framework utilizes the resource-based theory to link various classes of risks to an extended set of organizational resources.

Design/methodology/approach – The paper opted for an exploratory study using a sample from an online survey. The survey subjects were recruited from the membership database of the American Institute of Certified Public Accountants, focusing primarily on CFOs. The survey consisted of six sections: demographics, a section on each of the four risk types included in ERM: strategic risk, operational risk, financial risk and hazard risk, and exit questions (where very general questions about ERM were asked). The survey yielded a data set of 227 valid responses.

Findings – Using the associated sample survey data, the paper provides empirical validation of the proposed framework that managers in any organizations could use to identify and manage risks.

Research limitations/implications – The proposed model does have limitations that predominantly exist from the fact that human judgment in decision-making is not always data-driven, and hence, a proper risk exposure could be ignored based on pure arguments of cost and benefits from domain experts. Therefore, researchers and practitioners are encouraged to test the proposed framework further.

Practical implications – Risk exposure is not a snapshot event in an organization's time horizon. Rather, risk identification is an ongoing process and the proposed framework allows organizations to handle increasing complex risks and/or identifying them based on how the organizational resources may be exposed over time. Managers could use a form of risk control analytics (monitoring dashboard of all identified risks under each interaction sets on a regular basis) to become more proactive in managing risk or exploiting opportunities across enterprise.

Originality/value – This paper fulfills an identified need to study how enterprise risks exposure can be proactively assessed and managed.

Keywords Resource based theory, Risk identification, Strategic risk, Enterprise risk management, Exposure points, Interaction points

Paper type Research paper

Managerial Auditing Journal
© Emerald Publishing Limited
0268-6902
DOI 10.1108/MAJ-12-2017-1751

Introduction

Risk management is an important activity for organizations that are striving to provide value for their stakeholders in the face of real-world uncertainties. Efficient risk management could potentially present value-creating opportunities that may not have been identified otherwise. For a number of years, organizations have been attempting to identify and manage the risks inherent in their operations. The perceptions were that risks could result in negative events. Certain risks, such as hazard risks, are often addressed though insurance. Financial risks are dealt with by modifying business exposure such that the risk was minimized or avoided or through a transfer of the risk, or with hedges against risk exposure. The heightened awareness of the operational and strategic risks in recent years has demonstrated the increasing complexity of managing risks. These risks have the potential to add tremendous value to the organization when appropriately managed, while failure to manage them properly can vastly damage or even the cause demise of the organization.

Organizations are constantly examining their enterprise risk management (ERM) systems and are often particularly motivated by publicized failures of organizational risk management such as in Volkswagen, Enron, AIG and BP. In addition, risk exposure identified in the aftermath of natural catastrophes such as Katrina also drives new ERM effort. Regulators, corporate governance oversight bodies, rating agencies, investors and stock exchanges have increased the pressure for swift action to cure many of the perceived weaknesses in ERM. ERM has been elevated to much higher levels of management so that risks are managed across the enterprise, but actual practice varies greatly across organizations and industries. In addition, ERM practice has also been expanded to exploiting risks as opportunities.

Within ERM, the issue of risk identification still remains a fragmented area. That is, attempts to classify risk into categories, or dimensions, seem to be pursued by a variety of stakeholders, but those various stakeholder views have not been synthesized into a coherent view of risk. ERM attempts to provide a coherent view for managing risk, but several difficult questions remain about how to properly anticipate, plan and manage risk, and as such, ERM does not give a comprehensive answer as to how to think about, or map, risk in a structured or semi-structured manner. Without stronger guiding frameworks, effective and efficient risk identification and management are difficult. In this study, we investigate factors that influence ERM. We propose a framework for explaining the components of ERM by developing and testing a strategic risk identification framework. This framework would contribute to the proper development of the firm's total risk profile and may also constitute a strategic dynamic capability for an organization. There are three principal questions addressed in this study:

RQ1. What are the major risk issues or dimensions? More specifically, have we identified the right risks?

RQ2. Are the risk dimensions viewed as being linked to organizational resources? More specifically, does the proposed ERM framework protect organizational resources or create value for managers?

RQ3. Do organizations have sufficient incentives for practicing adequate ERM?

To address these questions, our strategic framework helps with understanding the interactions between risk classes and resources, as well as intra-resource interactions. Our

approach may lead to the development of one or more sustainable competitive advantages, in addition to protecting the organizational resources of the firm.

Theoretical positioning

Risk and the resource-based view

The resource-based view (RBV) of the firm postulates that a firm earns a competitive advantage over its market rivals by controlling and utilizing a unique set of resources (Barney and Hesterly, 2006). These resources would then be configured in such a way that the firm's customers would perceive the firm's resulting products or services as offering value. Given that a firm's competitors may eventually desire to pursue a similar strategy, the resources developed by the initial firm must be such that they cannot be duplicated efficiently by competitors nor can the competitors develop substitutes that could undermine the firm's advantage provided by these unique resources. If the unique conditions persist over time, then the firm initiating the strategy is said to have achieved a "sustainable competitive advantage", and it should earn an above-average return or "economic rent" (Barney and Hesterly, 2006). Barney (1991) defines resources as *all assets, capabilities, organizational processes, firm attributes, information, knowledge, etc. controlled by a firm that enable the firm to conceive of and implement strategies that improve its efficiency and effectiveness.* A more recent recognition has been formed around the view that even "resources" that are outside of the firm's direct boundaries also should be included in the resource base of the firm – this is known as the extended RBV (Mathews, 2003). The extended resources include not only internal resources, such as personnel, facilities and processes, but also customers, suppliers and other important outside entities like government entities, control bodies and geography. These resources are not only the elements that may help create a competitive advantage for a firm, but they also are the potential sources of risk exposure. The central idea of this paper is to base the identification of risk on the firm's extended resources via exposure points.

As noted in Eisenhardt and Martin (2000), dynamic capabilities "are the organizational and strategic routines by which firms achieve new resource configurations as markets emerge, collide, split, evolve, and die". While a basic capability allows the firm to utilize multiple resources to produce a result (Amit and Schoemaker, 1993), a dynamic capability allows the modification of these basic capabilities (and other organizational resources) to adapt to rapid market and organizational changes (Cepeda and Vera, 2007). Examples of dynamic capabilities include creation of new products (or services), risk minimization, alliance formation and strategic decision-making (Eisenhardt and Martin, 2000). We note that managing risk then can be viewed as a dynamic capability, which is shaped by the firm's resources and which also shapes the future organizational resources. Thus, risk identification is a potential dynamic resource that impacts the resources of the firm. The lack of this dynamic capability is unfortunately most often pointed out after a major event strikes. Examples include Volkswagen's failure to produce a 2l diesel engine that passes EPA and European emissions standards (2015), BP's oil spill in the Gulf of Mexico (2010), FEMA's preparedness for hurricane Katrina (2005) and London Whale trading loss at JP Morgan Chase in 2012. Clearly, there was a lack of managing the risk associated with certain organizational resources in these cases. Specifically, Volkswagen failed to ensure that one of their major resources, diesel engine production, was compliant with respect to emissions standards. Engine production is a major operational resource for an automobile manufacturer, as engines are typically used in many models over many years, including in the organizations various brand labels (like VW and Audi). In this paper, we propose a risk

identification framework that would indeed contribute to making ERM a dynamic capability.

ERM practice

Various professional and academic disciplines, like accounting, management, finance and actuarial science, have proposed their own methods, frameworks and classifications used for analyzing risk. For the stakeholders preparing, auditing or using accounting information for listed companies, the Sarbanes–Oxley Act (SOX) of 2002 has significantly changed the organizational landscape. The roles of management and auditors have become more complex and encompassing. Section 404 of SOX puts the onus on management to identify, document and evaluate significant internal controls. Internal controls are measures developed by an organization such that business is operated efficiently and according to policies and plans; to safeguard assets and resources; to detect fraud, theft and material errors; and to produce reliable financial and management information from accurate and complete accounting data. The organization's information and computer-based systems are becoming more sophisticated and multifaceted, thus adding to the complexity of the system of internal control.

Similarly, Section 409 of SOX entails rapid and current disclosure of material changes in an organization's financial conditions. Compliance with Section 409 of SOX implies that the management has the requisite legal, technical and financial expertise to produce financial information that is timely, reliable, consistent and objective. Auditors then have the responsibility to audit and report on the management's assertion about the strengths and weaknesses of the organization's system of internal controls.

Underlying these internal control measures are a number of risks such as information security risks, fraud risk, and systems security risk. Management accountants are in the forefront of this evolution and are using and evaluating complex information systems necessary to provide information for managerial decision-making. They have the responsibility that new information systems have the necessary features, such as controls and ability to store, access and retrieve information, as well as providing sufficient audit trails. The internal controls must be designed such that information systems are protected from a variety of risks. Defining, recognizing and controlling for these risks may influence the very survival of a firm in a competitive global marketplace, and the increasing amount of details seen in the supporting frameworks, such as Casualty Actuarial Society (CAS, 2011), the Committee of Sponsoring Organizations (COSO, 2004, 2016) and the International Standards Organization (ISO-31000, 2009), indicate that ERM practice is growing increasingly complex.

The Committee of Sponsoring Organizations (COSO, 2004) ERM Framework is an expansion of its internal control system and is geared to achieving four objective categories – strategic, operations, reporting and compliance. These four objectives are integrated with eight interrelated components, which are: the internal environment, setting objectives, identifying events, assessing risk, responding to risk, control activities, information and communication and risk monitoring. According to the COSO view, an entity's ERM is considered effective if the eight components are present and functioning effectively. When the eight components are effective in each of the four objective categories, then it is presumed that management and the board should have reasonable assurance that they understand the extent to which the entity's strategic and operations objectives are being achieved. It is also presumed that they should have reasonable assurance that the entity's reporting is reliable, and that the entity is in compliance with applicable laws and regulations. Operational risk is

the focus of the COSO risk management process and emphasizes clearly the various stakeholder dependent views of facets of operational risk.

Recently COSO (2016) proposed an updated framework to its COSO (2004) study to address the evolution of enterprise risk management and the need for organizations to improve their approach in managing their risk in today's business environment by recognizing the increasing importance of the connection between strategy and enterprise performance. The new COSO Public Exposure Draft framework proposes a smaller set of principles organized in five related components supported by 23 principles (or sub-components) that support the five components as follows:

(1) *Risk governance and culture*: Exercises board risk oversight, establishes governance and operating model, defines deferred organizational behaviors, demonstrates commitment to integrity and ethics, enforces accountability, attracts, develops and retains talented individuals.

(2) *Risk, strategy and objective setting*: Considers risk and business context, defines risk appetite, evaluates alternative strategies, considers risk while establishing business objectives, defines acceptable variation in performance.

(3) *Risk and execution*: Identifies risk in execution, assesses severity of risk, prioritizes risk, identifies and selects risk responses, assesses risk in execution, develops portfolio view.

(4) *Risk information, communication and reporting*: Uses relevant information, leverages information systems, communicates risk information, reports on risk, culture and performance.

(5) *Monitoring ERM performance*: Monitors substantial change, monitors ERM.

Taking a more macro, or process, view of risk, the International Standards Organization (ISO-31000 2009) specifies a risk management process in seven steps (Figure 1):

(1) *Establish context*, that is, understanding the current conditions in which the organization operates.

(2) *Identify risks*, which includes documentation of threats and opportunities impacting the organization.

(3) *Analyze/quantify risks*, which includes estimating outcomes for each material risk.

(4) *Evaluate risks*, which includes aggregation, analysis and projected impact on the organization's performance metrics (and therefore, the risks' priority).

(5) *Treat risks*, which includes plans for controlling and exploiting the various risks.

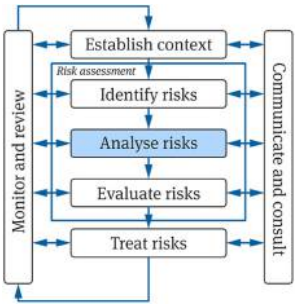


Figure 1.
The ISO 31,000 ERM process

(6) *Monitor and review*, which includes measurement and monitoring and feedback to the risk management strategies.

(7) *Communicate and consult*, which, along with monitor and review, are continuing efforts in parallel to Steps 1 through 5 above.

It seems that the various frameworks for risk management are somewhat converging, but that these approaches also call for methodologies to help establish both risk contexts and identification. This paper will, therefore, build on prior practice and focus on the issues of establishing context and identifying risks using the aforementioned new strategic framework.

ERM research

In the last decade, there have been hundreds of papers published related to descriptions and operational aspects of ERM. Recent academic research has been published that reports on many issues related to the dynamics of implementation, decision-making and control aspects of ERM and also whether an ERM program adds value to the firm.

Many factors have been studied related to the dynamics of ERM implementation. These dynamic factors include those associated with the extent of implementation of ERM. For example, Beasley and Hermanson (2005) gathered data from 123 organizations and found that the stage of ERM implementation is positively related to the presence of a chief risk officer, board independence, CEO and CFO apparent support for ERM, the presence of a Big 4 auditor, entity size and entities in the banking, education and insurance industries.

A case study by Arena *et al.* (2010) was utilized to analyze the organizational dynamics surrounding the implementation of ERM. A field study was carried out over a seven-year period from 2002 to 2008 in three private organizations. The authors state that their 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. Finally, the authors contend their work provides evidence supporting a holistic research approach that considers the behavior of people and their interrelations, along with technological solutions as they occur in historical events and cycles.

Research by Drew *et al.* (2006) looked at the nature of risk and considers how such risk is defined, classified, measured and framed. Multiple forces that shape risk exposure in forms and how these forces may interact and change. They identified the cognitive and other biases that typically confound decision-making. The critical organizational factors for implementing and integrated approach to risk management were explained. These factors include the five pillars of corporate governance – culture, leadership, alignment, structure and systems.

A study by von Känel *et al.* (2010) established three conceptual frameworks that provide a basis for an enterprise embarking on ERM:

- a risk management cycle that provides a discipline to consistently and coherently manage virtually all of the risks of the enterprise;
- a risk-related taxonomy that provides a foundation for clear and concise communication about risk across the enterprise to enable better risk management; and
- an ERM maturity model and its associated capability assessment to allow an organization to determine gaps in its current management process and define ways to improve those ERM capabilities.

The authors contend that these three frameworks together are key enablers for a successful ERM implementation and ongoing operation.

Also, Gates (2006) used data collected from a survey of 271 risk and financial executives to explain why ERM has become a priority, including the benefits being reported by early adopters and challenges faced by companies implementing ERM. It also considered the question of the optimal "owner" of the ERM process that would encourage strategic risks to be identified and managed in an integrated framework. This exploratory investigation looks at the main drivers and benefits of, and remaining obstacles to, the new corporate practice of ERM.

The relationship between organizational culture and ERM combined a cultural measurement instrument (organizational cultural assessment) with gauges of ERM implementation were studied by Kimbrough and Componation (2009). Their study attempted to test whether or not there is a significant relationship between an organization's score on the organizational cultural assessment and its score on metrics reflecting the degree of ERM implementation. Their analysis supports the hypothesis that organic cultures tend to make greater progress in their ERM programs.

As to decision-making and control areas, research has reported on incorporating risk management into the financial planning process through a budgeting process (Alviniussen and Jankensgard, 2009). The authors present a quantitative approach to risk management that retains the integrative, enterprise-wide mindset, yet equips corporate management with the ability to evaluate financial distress probabilities by incorporating ideas related to the concept of a firm's economic capital. This effort is termed enterprise risk budgeting (ERB). ERB entails using quantitative modeling in the corporate-level financial planning process. This model enables an ongoing assessment of the expected financial situation and risk profile of a company.

As to other operational decisions, such as the risks associated with outsourcing, Beasley *et al.* (2004) point out that outsourcing can create risks to an enterprise's strategy, market, operations, finance, human capital, IT, legal/regulatory and reputation. The authors call attention to the fact that not only should these risk exposures be evaluated and monitored across the enterprise, but their interactive or cumulative effect must also be managed on a portfolio basis.

In another closely related issue, Shah (2009) focused on the supply chain risk management process, and in particular on identifying and mitigating supply-side risks related to price and supply chain disruptions, as well as and managing supply-side risks through judicious use of efficient and responsive chains. The proposed process also included the identification of supply- and demand-side risks in an environment of high uncertainty. Such a process should help companies develop effective risk management plans.

Also related to supply chain risks, the function of vendor selection was also the subject of research using a data envelopment analysis (DEA) value-at-risk (VaR) model as a new tool to conduct risk management (Olson and Dash Wu, 2010). This paper demonstrated how VaR modeling could apply in supply chain management as a simplified version of existing stochastic DEA models. The DEA/VaR approach offers a tool to perform efficiency analysis by handling both inefficiency and stochastic error.

A study of ERM and ethics by Weitzner and Darroch (2010) explored the link between strategic goals, ERM and ethics with the goal of offering a practical framework for managers evaluating ethical dilemmas. The authors argue that the firm, as a strategic decision, must decide its own ethical norms and recognize that certain decisions must be ethically based not strategically based. They also argue that the firm may be forced to set boundaries between the role of the private sector and civil society or the public sector.

There have been several studies attempting to assess the value to the firm and to shareholders of adopting ERM. In Smithson and Simkins (2005), four specific questions were posed in a survey to determine whether there is evidence that risk management increases the value of the firm. The authors found that the bulk of evidence supports the idea that risk management adds value.

A study by Beasley *et al.* (2008) showed less definitive results of the costs and benefits of ERM when evaluating a market response to hiring announcements of senior executives overseeing enterprise-wide ERM processes. The authors' test was based on a sample of 120 announcements of such hiring from 1992 to 2003. Other tests in this study suggested that costs and benefits of ERM may be firm-specific.

Based on a test sample of 112 US firms that disclosed ERM activities in 10Ks and 10Qs, the findings by Gordon *et al.* (2009) provide strong evidence that there is a positive relation between ERM and firm performance. This relation is contingent upon the appropriate match between a firm's ERM system and five factors affecting the firm: environmental uncertainty, industry competition, firm size, firm complexity and board of directors' monitoring.

In a recent paper, Shad and Lai (2015) propose an implementation framework for ERM that captures the casual relationships of the risks that are strategically associated with a firm's business performance, as well as the cost of capital. In their framework, they show that shareholder value is created by way of lowering the corporations' cost of capital, which takes place through a risk premium reduction mechanism, and they further argue that value is created by means of a generic improvement of business performance.

A strategic view of risk management

It is apparent that both the applied frameworks and some of the research summarized above have a strong focus on providing procedural guidelines for managing risk in the enterprise. A broader view, and an apparent trend in practice, is to look at the context of the ERM process from a more strategic perspective. Figure 2 shows the ERM process itself as specified in the ISO 31000 standard and also illustrates that the process is impacted (or influenced) by both a resource system and an incentive system, to create value for the firms. The capabilities, in the context of ERM, are those that are developed in connection with the ISO 31000 process. These capabilities are only going to be developed if there is a resource system present, which provides the necessary resources for development, and there is an

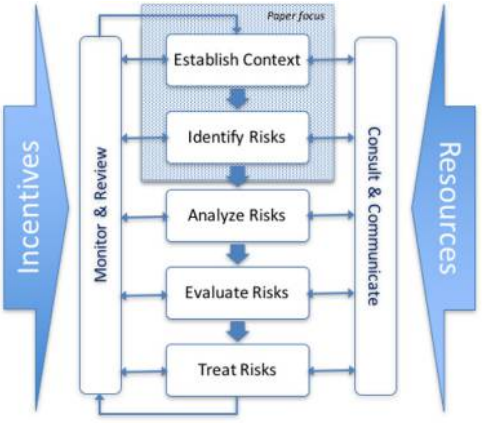


Figure 2.
Strategic view of ERM processes

incentive system present, which provides the needed incentives for action. Clearly, SOX provides such an incentive at a high level, but also more direct incentives could be present (such as direct performance incentives). Our research also raises the question whether there is a lack of direct incentives for risk management in organizations.

Toward a formal definitions of risk

While terms related to risk and ERM are found in a variety of academic and managerial publications, no collective view of these risk terms have been proposed to our knowledge. As such, we first propose a series of definitions: We define ERM as *the methods and processes used by organizations to manage risks on an enterprise-wide basis and seize opportunities related to the achievement of their objectives*. Within this view, risk is viewed as a concept that denotes a potential *negative impact* to firm value that may arise from a future event, while effective and efficient management of risk can lead to competitive advantage for firm. Thus, risk can be a *potential opportunity* that, if properly managed, may enhance the value of the firm. Based on the academic and professional literature surrounding risk analysis, a set of four broad classes of risk with associated definitions seem to have broad acceptance, but are, to the best of our knowledge, never before proposed as comprehensive risk classes. These are as follows:

- *Strategic risk*: A broad class of risk that has potential negative impact on the achievement of a firm's strategic objectives.
- *Operational risk*: Risk arising from a company's business functions and from the practical implementation of the management's strategy. This includes products and services, financial measurement and reporting risk, fraud risk and IT risk.
- *Financial risk*: Risks associated with pricing, currency, credit, liquidity, market, solvency and assets.
- *Hazard risk*: Risks associated with nature (including earthquakes, hurricanes, tornados, flood, fire, drought) and risks related to terrorism and political unrest (including riots, hijackings and strikes).

We note that Lam (2014) discussed three of these risk classes (strategic, operational and financial), and the risk classes sometimes overlap in nature. In our model, we address hazard risk as well, and we next show how these four risk classes are linked to the firm's resources.

A framework for risk identification

While the frameworks by CAS, COSO and ISO provide a roadmap for ERM, they lack the ability to view elements that impact risk in a resource-focused manner. Instead, we argue that all classes of extended organizational resources should be viewed as potential sources for, or exposure to, risk. A resource may be exposed to all four proposed classes of risk. Thus, the potential interaction between a resource (category) and a risk class must be considered – we label this an "interaction set", as for each risk class, there may be several resources of a particular category that may be exposed to a risk of a certain type. Thus, our proposed framework offers a perspective which helps identify organizational exposure points that typically emanate from the extended resources that an organization controls, and which may lead to exposure to risk. These extended firm resources, that we call *interacting resources*, can broadly be classified as:

- personnel and structure (human resources and its organization);
- processes and plans;

- facilities and operational assets (including technologies);
- customers and suppliers; and
- external (such as regulatory bodies and organizations).

Linking organizational resources to risk categories provides a natural way to study ERM, and this RBV of organizational challenges was first proposed in Rolland *et al.* (2009) and utilized also in Mishra and Rolland (2009). It is our view that these five interacting resources categories cause risk exposure by triggering events that emanate from one of the four major risk classes (strategic, operational, financial and hazard). To better aid managers to think about, and anticipate risk, we therefore link the *interacting resources* to the risk classes in a framework as depicted in Figure 3. Shown in this figure are in total 20 interaction sets that could encompass zero of more interaction points, where a particular resource is exposed to a particular risk. In other words, an interaction set is found at the intersection of an interacting *resource* and a *risk class*. Each interaction set may include a variety of interaction points (IP). The IPs are meant as placeholders for whom or what (in terms of resources) are "causing" or associated with the particular risk class. For example, under strategic risk and plans and processes, one possible interaction point is related to the existence of organizational processes/plans for managing reputational risk. Similarly, strategic risk/customers and supplier, an interacting issue, would be contingencies for managing supply chain disruptions. The reasoning behind the framework is to generate a tool that allows managers to think along certain guidelines (the interacting resources) about what/who is related to what type of risk class and their interdependencies. The framework should also allow managers to think rationally and expansively about risk management. This framework may constitute a strategic, dynamic capability for the organization and may contribute to the proper development of the firm's total risk profile and the minimization of risk exposure. Beasley *et al.* (2011) propose a method which links strategic initiatives to potential risks and propose associated key risk indicators and possible strategic responses. Our method takes a different approach to risk identification by linking risk classes to key resources of the

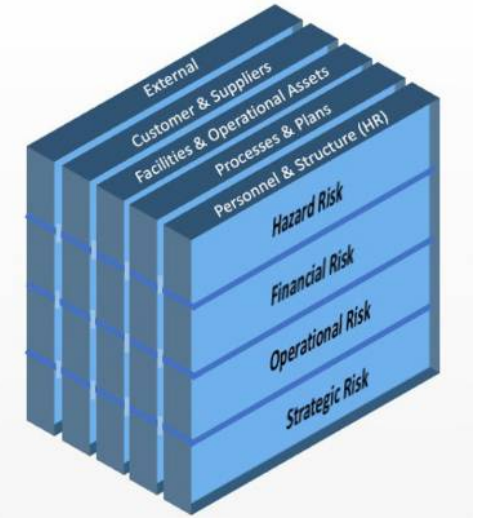


Figure 3.
A strategic framework for ERM and identification

organization. Once the risks are identified, the Beasley *et al.* (2011) framework can be used to identify key risk indicators and possible strategic responses.

Risk typically will increase if the exposure points are not managed. An illustrative example or how risk can be found in the Jerome Kerviel – Société Générale fraud case, where de-provisioning information access rights did not occur, resulting in violation of a fundamental internal control principle, separation-of-duty and eventually to a loss for the bank of more than US$7bn[1]. Indeed, the exposure points were not managed at all in this case, and the fraud went unnoticed until external control measures exposed irregularities. For the recent Volkswagen engine emission crisis, an operational resource (the 2l diesel engine manufacturing process, or the 2l diesel engine as a product itself) interacted with an external resource (emissions control agencies such as the EPA), exposing the organization to a liability related to all cars sold with such an engine, indeed exposing multiple brand labels (i.e. Volkswagen, Audi and Porsche).

We note that the goal of our framework presented in this paper is to identify the IPs between the risk classes and organizational resources and their potential interdependencies. Once identified, many of these risks can be managed using methodologies from finance, statistics and mathematics. For a comprehensive overview of such methods, please refer to McNeil *et al.* (2015).

Validating the framework

We designed a study to examine factors influencing ERM in the context of the above proposed framework. The research was conducted as a part of the management accounting research series, sponsored by the American Institute of Certified Public Accountants. The survey consisted of six sections: demographics, a section on each of the four risk types included in ERM: strategic risk, operational risk, financial risk, and hazard risk and exit questions (where very general questions about ERM were asked). Below we describe the details of methodology and data collection procedure.

Methodology and data collection

To test the framework, a set of IPs were developed that were consistent with past risk research and consistent with several experts' and managers' views of what might be some possible IPs. As such, groups of questions were developed that could be answered by using relatively simple Likert scale responses. We used a five-point scale with the following scale items: strongly agree (SA), agree (A), neutral or no opinion, disagree (D) and strongly disagree (SD). The detailed survey questions related to the interacting resources and risk categories are found in Appendix 1.

The additional questions presented from the survey tool are related to demographics, risk metrics and other outcome variables and are listed under the heading "Exit Questions". Primary questions in this section addressed the overall importance of these IPs to organizations' ERM as seen from the organization's (CFO's) perspective and to what extent organizations are addressing these IPs identified by the framework.

Data were collected during the spring of 2009 through an online survey instrument electronically sent to members of the AICPA's business and industry group who serve in chief financial officer or equivalent positions. The respondents completed the online survey with questions that address factors related to ERM within their organization. They were asked 38 questions related to ERM, organizational resources and risk types that their organizations are faced with. The survey participants are members of AICPA, and the survey was conducted under the auspices of AICPA. The survey participation was voluntary.

While our survey was conducted during 2009, it is instructive to note that our effort is purely to validate our model based on an extended resource-based theory and comprehensive classification of risk types. We use the interaction set points as a fundamental basis to identify the different risks that a firm is likely to be exposed to. The framework is validated using a survey methodology which in principle should be completely time-independent. In other words, the framework itself does not change with time or the perception of a particular type of risk being high or low. It is interesting to note that perception of risk is different for different type of firms at any point of time. For example, while war is bad for general economy, it can be good for firms operating in defense industries. Similarly, different firms may suffer from different type of hazard risk, such as cyclones, flood and earthquake, whose intensity varies during the season. Therefore, we believe that, while our survey was done after the 2007-2008 financial crisis, the timing should not affect our overall results as the framework is time invariant.

Among the respondents 83.2 per cent reported holding positions as chief financial officers and 5.6 per cent hold the title of controller. Other respondents held titles as treasurer (1.7 per cent), CEO/president and chief risk officer (both at 1.1 per cent). Of the respondents, 0.6 per cent reported title as head of internal audit and 6.7 per cent held other positions.

Of the respondents, 54.2 per cent work for privately owned US companies. The next largest group is government, education and not-for-profit (21.8 per cent), followed by US public companies (13.4 per cent) and foreign-owned companies (7.8 per cent). Of the respondents, 2.8 per cent reported other (unknown) ownership structures.

The majority of respondents (80.4 per cent) work for companies with US$10m or more in annual revenues. Approximately 96.6 per cent of the respondents work for companies with more than 10 employees. The largest industry groups represented in this survey are finance and insurance (19.6 per cent), manufacturing (19 per cent), followed by health care and social assistance (8.4 per cent) and construction (7.3 per cent).

In total, we received 227 fully or partially completed surveys, and the complete survey results are found in Appendix 2.

Descriptive analysis of risk class and interaction points

In this section, we discuss the detail results from our survey as it pertains to interaction of the four risk classes as seen in Figure 2: strategic risk, operational risk, financial risk and hazard risk; with the five organizational resources: (A) personnel and structure, (B) process and plans, (C) facilities and operational assets (technologies), (D) customer and supplier and (E) external as identified under extended RBV. The goal is to understand both the individual interaction of risk classes with firm's recourses, as well as the variation of the nature of interaction across the risk classes.

For a given risk class, answers to our survey questions (regarding a risk from a particular organizational resource) were pooled in five different categories: 1. strongly agree, 2. agree, 3. neural, 4. disagree and 5. strongly disagree. A box-and-whisker plot was used to depict the differences between these five groups that varied in their responses. For each of the four risk classes and five organizational resources, the process was repeated so that these five levels of responses can be analyzed simultaneously. Further, the mean value of the response rates was used to test the proposed framework. As shown in the Figures 4-7, the responses are highly in favor of our framework. In all four risk classes, overall, more than 60 per cent of the respondents either agree or strongly agree with the risk generated from five basic resources (A: personnel and structure, B: process and plans, C: facilities and operational assets, D: customers and suppliers and E: external) proposed by our framework (Figure 7). The spread in data (box-and-whisker plot) for each resource and risk class comes

from the fact that slightly different responses were received when different questions were used to capture the same interaction.

Results from reliability test

The Cronbach's α reliability test was done to evaluate the extent to which our question or pool of questions captured each of the interaction sets (or constructs) in the model. Internal consistency between the survey questions describes the extent to which all the questions in the test measure the same construct. Below is the summary of the results obtained from the

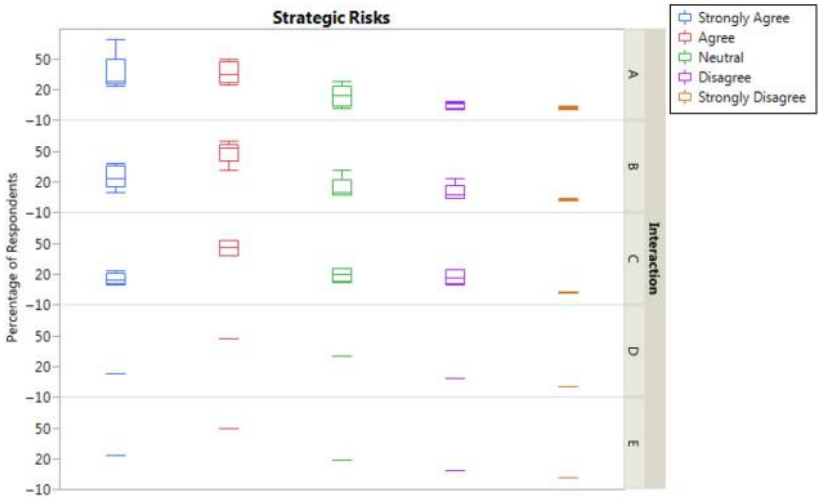


Figure 4.
Survey results from 227 respondents who shared their experience on their organization's approach to mitigate strategic risk and how they perceive the related resources contributing to the process

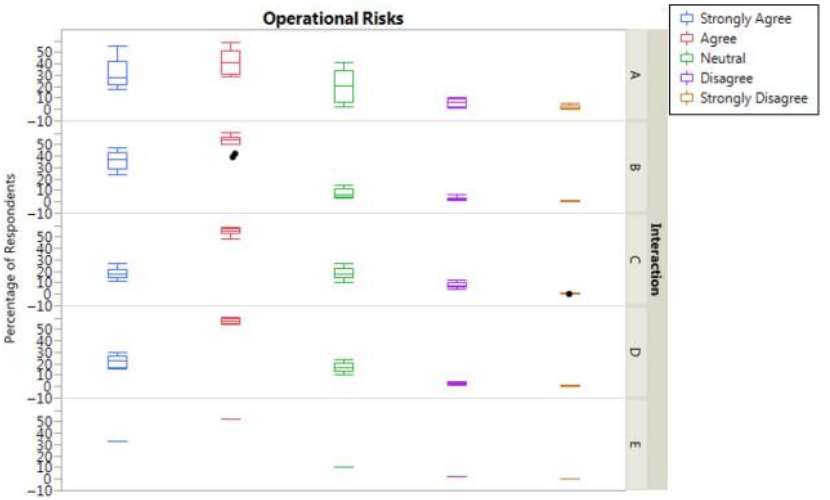


Figure 5.
Survey results from 227 respondents who shared their experience on their organization's approach to mitigate operational risk and how they perceive the related resources contributing to the process

test. Table I. A reports the questions associated with each interaction construct per our survey design intentions.

For each test, we had about 200 responses from a pool of two to eight questions (as in Table I). We did not perform Cronbach's α test for response categories with only one question in the construct (shown in the Table II as n/a). Most of the tests show α value to be more than 0.8 which suggests that there is 0.36 or less error variance (random error) in the score. [1 – 0.8 * 0.8) = 0.36]. We further investigated the three constructs with slightly lower α (0.605 ~ 0.643) to understand a potential source of internal inconsistency in the survey questions. We argue that the resource "Personnel and Structure" covers a wide personnel

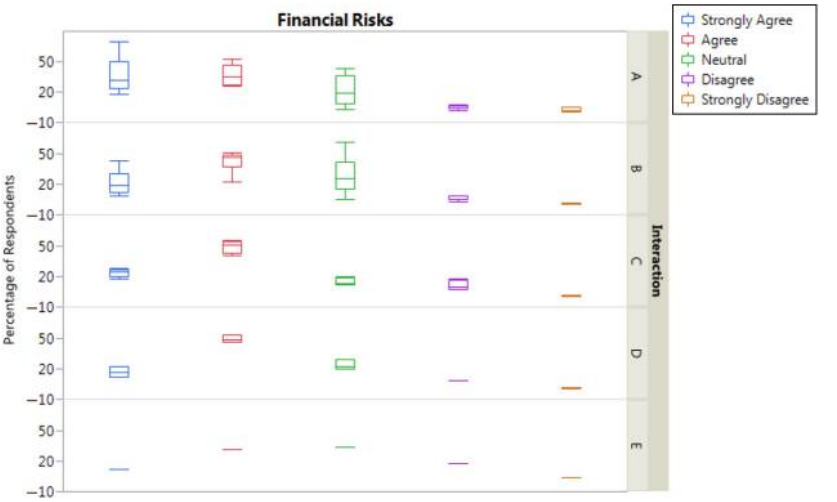


Figure 6.
Survey results from 227 respondents who shared their experience on their organization's approach to mitigate financial risk and how they perceive the related resources contributing to the process

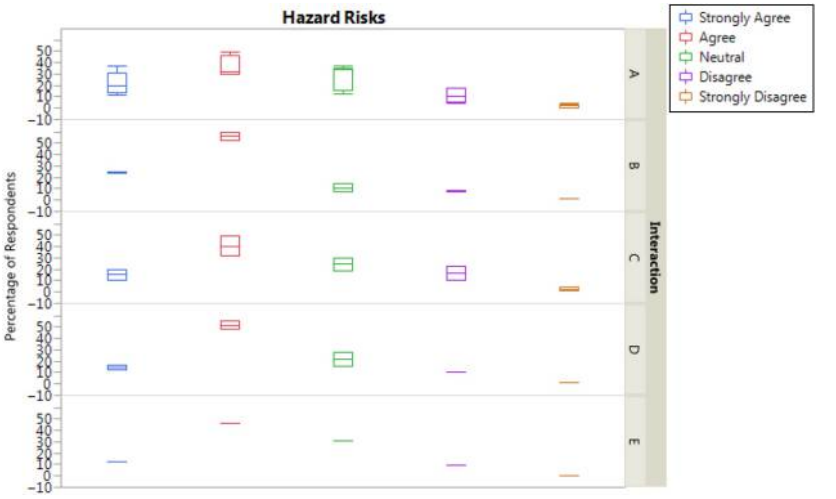


Figure 7.
Survey results from 227 respondents who shared their experience on their organization's approach to mitigate hazard risk and how they perceive the related resources contributing to the process

portfolio such as directors, managers, executives and risk professional and might have led to different perceptions for different responders, and hence diluting the consistency. A further dimensionality test on the same pool of resources could not direct us to a conclusion otherwise.

Hypothesis test for overall enterprise risk assessments

At the end of the survey, each of the responders was asked the following question: "Q38: Do you believe this survey adequately addresses the different aspects of enterprise risk management? Please provide any comments that may improve the survey". We divided their responses into two different categories: (1) agreed + strongly agreed and (2) neutral, disagree and strongly disagree. From the survey sample, we want to test that the response is not biased toward one of the two categories. Our null hypothesis states that the proportion ("Agreed + Strongly Agreed" to "All Response") is less than equal to 0.5 for the entire population. We believe this proportion should be more than 50 per cent to justify the overall strength of the model.

As shown in Table III, with a significance level of 95 per cent, we reject the null hypothesis, and this provides further evidence of the validity of our model, and that the survey-takers were not indifferent.

The survey responses were further analyzed by categorizing responses in two groups:

(1) the number of responses that agreed or strongly agreed; and

(2) the number of responses that were neutral, disagreed or strongly disagreed in their answer to each question.

The percentage of agreed and strongly agreed is given in Figure 8 below.

Table I. Relationship between the survey questions and the interaction sets

	Personnel & structure	Processes & plans	Facilities & operational assets	Customers & suppliers	External
Strategic Risk	Q1 a- e	Q2 a- c, Q3 a- b	Q4 a-d	Q5f	Q5g
Operational Risk	Q7 a- e	Q8 a-c	Q10 a-f	Q11 a-e	Q12
Financial Risk	Q14 a- e	Q15 a- c, Q16 a-c, Q17 a- d	Q18 a-d	Q19 a- c	Q20
Hazard Risk	Q22 a-e	Q23 a-b	Q23 c, Q24 a	Q25 a-b	Q26

Table II. Cronbach alpha for the interaction sets

Risks\Resources	A: Personnel & structure	B: Process & plans	C: Facilites & operational assets	D: customer & suppliers	E: External
Strategic risk	*0.605*	0.801	0.837	n/a	n/a
Operational risk	*0.643*	0.911	0.846	0.782	n/a
Financial risk	*0.643*	0.868	0.873	0.808	n/a
Hazard risk	0.755	0.903	n/a	0.872	n/a

Table III. t-Test for Indifference of model

Binomial test	Level tested	Hypoth Prob (p1)	p-Value
Ha: Prob(p > p1)	S&A	0.50000	0.0002*

A proxy for validation of each interaction set would be that the proportion of positive answers (agree + disagree) to individual questions are statistically different from the negative and neutral answers. As an even more restrictive test, all interaction sets can be tested in this manner with one collective *t*-test. Thus, we performed a *t*-test to assess whether the means of two groups (positive vs neutral + negative) are statistically different from each other. The distribution of response difference between this two groups is shown in Figure 9.

From Figure 9, we conclude that the responses are significantly higher in the group of strongly agree or agree for 79 survey questions. Based on this sample survey, we conclude that our model is further validated with strong agreement by the survey responders to the questions that captures the proposed 20 interaction sets between risks and resources within an enterprise.

Results from factor analysis

We subjected the data set to a principal component analysis (PCA) to check whether we could identify a reduced set of latent variables on risk factors that share a common variance. These unobservable factors are hypothetical constructs that are used to represent certain

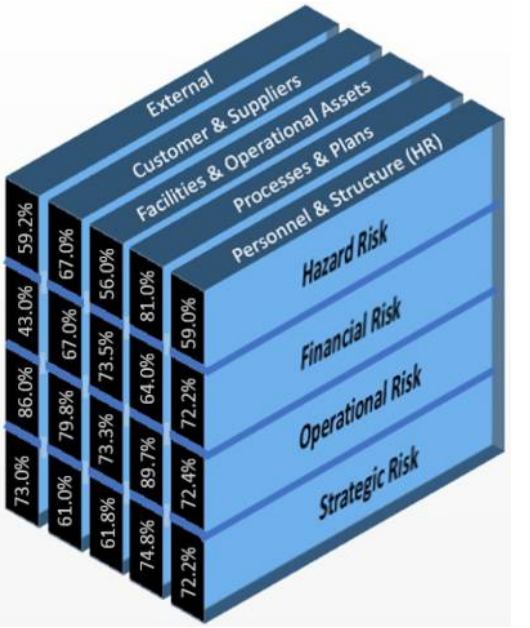
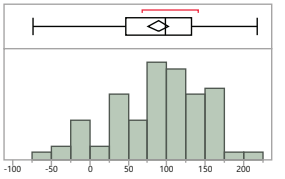


Figure 8.
Survey results (percentage of respondents from a total of 227 participants) who either agree or strongly agree on the organization's approach to mitigate four different classes of risks contributing from five different resources as perceived by the respondents



Mean	89.105481
Std Dev	60.852178
Std Err Mean	6.8464049
Upper 95% Mean	102.73563
Lower 95% Mean	75.475336
N	79

Hypothesized Value	0
Actual Estimate	89.1055
DF	78
Std Dev	60.8522

t Test	
Test Statistic	13.0149
Prob > |t|	<0.0001*
Prob > t	<0.0001*
Prob < t	1.0000

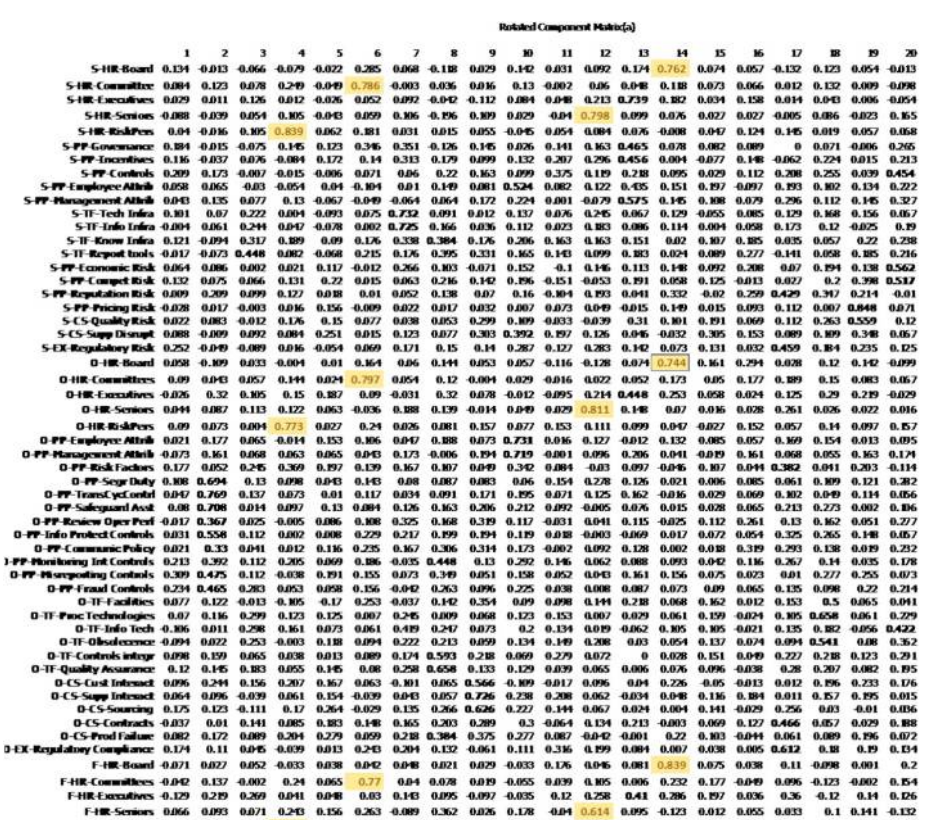
Figure 9.
t-test for indifference of overall interaction sets

variables. In summary, the PCA did not lead to direct insights with respect to reducing the latent variables. In fact, the PCA did not yield reasonable results with high loadings when reducing the factors below 20. The PCA results are depicted in Figure 10, and the following interpretations are drawn from studying various PCAs:

- Organizations are equipped with tools to mitigate hazard-related risks that might disrupt day-to-day operations. Managers use available technology and operational assets within the organizations to prepare and implement appropriate processes to tackle such risks.
- Internal control such as clear segregation of duty, implementation of control procedures, proper safeguards of assets, information protections protocol are part of the risk management processes and managers have incentive to put them in place to avoid risks related to process and planning.
- For financial risks, technological assets, infrastructures and information tools are implemented in the organizations by managers as appropriate risk management tools.
- Risk professionals are engaged in overall risk management for the organization.
- Specialty groups such as audit, budget and risk and corporate governance committee are actively engaged in strategic, operational and financial risk management in an organization.
- Organizations manage operational risks related to customer interactions, supplier interactions and procurement sourcing.
- Strategic and operational risks are managed by designing an effective control environment that considers management and employee attributes.
- Operational processes enable organizations to manage risks arising due to market liquidity, partner credit and equity.
- Senior managers and managers are actively engaged in managing risks coming from all four risk classes.
- Organization provides an appropriate governance structure for executives to get engaged in strategic, operational and financial risk management.
- The organization's board of directors are actively engaged in strategic, operational and financial risk managements. This is in line with recent research, as Aebi, Sabato and Schmid (2012) found that banks, in which a chief risk officer directly reported to the board of directors and not to the CEO, exhibited significantly higher stock returns and ROE during the recent financial crisis (2007/2008).
- Operational processes in place enable organizations to manage market risks.
- Specialty groups, executive managers and board of directors are actively engaged in hazard risk management.
- Organization manages operational risks related to office, production facilities, process technology responsible for competitive strategy and obsolescence of technologies and facilities.

Implications for research and practice

This paper is theoretically grounded in Barney and Hesterly's (1991) theory of the firm. We argue that the organizational resources, or "all assets, capabilities, organizational processes,



Rotated Component Matrix(a)

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
S-HR-Board	0.134	-0.013	-0.066	-0.079	-0.022	0.285	0.068	-0.118	0.029	0.142	0.031	0.092	0.174	0.762	0.074	0.057	-0.132	0.123	0.054	-0.013
S-HR-Committee	0.084	0.123	0.078	0.249	-0.049	0.786	-0.003	0.036	0.016	0.13	-0.002	0.06	0.048	0.118	0.073	0.066	0.012	0.132	0.009	-0.098
S-HR-Executives	0.029	0.011	0.126	0.012	-0.026	0.052	0.092	-0.042	-0.112	0.084	0.048	0.213	0.739	0.182	0.034	0.158	0.014	0.043	0.086	-0.054
S-HR-Seniors	-0.088	-0.039	0.054	0.105	-0.043	0.059	0.106	-0.196	0.109	0.029	-0.04	0.798	0.099	0.076	0.027	0.027	-0.005	0.086	-0.023	0.165
S-HR-RiskPers	0.04	-0.016	0.105	0.839	0.062	0.181	0.031	0.015	0.055	-0.045	0.054	0.084	0.076	-0.008	0.047	0.124	0.145	0.019	0.057	0.058
S-PP-Governance	0.184	-0.015	-0.075	0.145	0.123	0.346	0.351	-0.126	0.145	0.026	0.141	0.163	0.465	0.078	0.082	0.089	0	0.071	-0.006	0.265
S-PP-Incentives	0.116	-0.037	0.076	-0.084	0.172	0.14	0.313	0.179	0.099	0.132	0.207	0.296	0.456	0.004	-0.077	0.148	-0.062	0.224	0.015	0.213
S-PP-Controls	0.209	0.173	-0.007	-0.015	-0.006	0.071	0.06	0.22	0.163	0.099	0.375	0.119	0.218	0.095	0.029	0.112	0.208	0.255	0.039	0.454
S-PP-Employee Attrib	0.058	0.065	-0.03	-0.054	0.04	-0.104	0.01	0.149	0.081	0.524	0.082	0.122	0.435	0.151	0.197	-0.097	0.193	0.102	0.134	0.222
S-PP-Management Attrib	0.043	0.135	0.077	0.13	-0.067	0.049	0.064	0.064	0.172	0.224	0.001	-0.079	0.575	0.145	0.108	0.079	0.296	0.112	0.145	0.327
S-TF-Tech Infra	0.101	0.07	0.222	0.004	-0.093	0.075	0.732	0.091	0.012	0.137	0.076	0.245	0.067	0.129	-0.055	0.085	0.129	0.168	0.156	0.057
S-TF-Info Infra	-0.004	0.061	0.244	0.047	-0.078	0.002	0.725	0.166	0.036	0.112	0.023	0.183	0.086	0.114	0.004	0.058	0.173	0.12	-0.025	0.19
S-TF-Know Infra	0.121	-0.094	0.317	0.189	0.09	0.176	0.338	0.384	0.176	0.206	0.163	0.163	0.151	0.02	0.107	0.185	0.035	0.057	0.22	0.238
S-TF-Repost tools	-0.017	-0.073	0.448	0.082	-0.068	0.215	0.176	0.395	0.331	0.165	0.143	0.099	0.183	0.024	0.089	0.277	-0.141	0.058	0.185	0.216
S-PP-Economic Risk	0.064	0.086	0.002	0.021	0.117	-0.012	0.266	0.103	-0.071	0.152	-0.1	0.146	0.113	0.148	0.092	0.208	0.07	0.194	0.138	0.562
S-PP-Compet Risk	0.132	0.075	0.066	0.131	0.22	0.015	0.063	0.216	0.142	0.196	-0.151	-0.053	0.191	0.058	0.125	-0.013	0.027	0.2	0.398	0.537
S-PP-Reputation Risk	0.009	0.209	0.099	0.127	0.018	0.01	0.052	0.138	0.07	0.16	-0.104	0.193	0.041	0.332	-0.02	0.259	0.429	0.347	0.214	-0.01
S-PP-Pricing Risk	-0.028	0.017	-0.003	0.016	0.156	-0.009	0.022	0.017	0.032	0.007	0.073	0.049	-0.015	0.149	0.015	0.093	0.112	0.087	0.848	0.071
S-CS-Quality Risk	0.022	0.083	-0.012	0.176	0.15	0.077	0.038	0.053	0.299	0.109	-0.033	-0.039	0.31	0.101	0.191	0.069	0.112	0.263	0.559	0.12
S-CS-Supp Disrupt	0.088	-0.009	0.092	0.084	0.251	0.015	0.123	0.077	0.303	0.392	0.197	0.126	0.046	-0.032	0.305	0.153	0.089	0.109	0.348	0.057
S-EX-Regulatory Risk	0.252	-0.049	-0.089	0.016	-0.054	0.069	0.171	0.15	0.14	0.287	0.127	0.283	0.142	0.073	0.131	0.032	0.459	0.184	0.235	0.125
O-HR-Board	0.058	-0.109	0.033	-0.004	0.01	0.164	0.06	0.144	0.053	0.057	0.116	-0.128	0.074	0.744	0.161	0.294	0.028	0.12	0.142	-0.099
O-HR-Committees	0.09	0.043	0.057	0.144	0.024	0.797	0.054	0.12	-0.004	0.029	0.016	0.022	0.052	0.173	0.05	0.177	0.189	0.15	0.083	0.057
O-HR-Executives	-0.026	0.32	0.105	0.15	0.187	0.09	-0.031	0.32	0.078	-0.012	-0.095	0.214	0.448	0.253	0.058	0.024	0.125	0.29	0.219	-0.029
O-HR-Seniors	0.044	0.087	0.113	0.122	0.063	-0.036	0.188	0.139	-0.014	0.049	0.029	0.811	0.148	0.07	0.016	0.028	0.261	0.026	0.022	0.016
O-HR-RiskPers	0.09	0.073	0.004	0.773	0.027	0.24	0.026	0.081	0.157	0.077	0.153	0.111	0.099	0.047	-0.027	0.152	0.057	0.14	0.097	0.157
O-PP-Employee Attrib	0.021	0.177	0.065	-0.014	0.153	0.106	0.047	0.188	0.073	0.731	0.016	0.127	-0.012	0.132	0.085	0.057	0.169	0.154	0.013	0.095
O-PP-Management Attrib	-0.073	0.161	0.068	0.063	0.065	0.043	0.173	-0.006	0.194	0.719	-0.001	0.096	0.206	0.041	-0.019	0.161	0.068	0.055	0.163	0.174
O-PP-Risk Factors	0.177	0.052	0.245	0.369	0.197	0.139	0.167	0.107	0.049	0.342	0.084	-0.03	0.097	0.046	0.107	0.044	0.382	0.041	0.203	-0.114
O-PP-Segr Duty	0.108	0.694	0.13	0.098	0.043	0.143	0.08	0.087	0.083	0.06	0.154	0.278	0.126	0.021	0.006	0.085	0.061	0.109	0.121	0.282
O-PP-TransCycCondtl	0.047	0.769	0.137	0.073	0.01	0.117	0.034	0.091	0.171	0.195	0.071	0.125	0.162	-0.016	0.029	0.069	0.102	0.049	0.114	0.056
O-PP-Safeguard Asst	0.08	0.708	0.014	0.097	0.13	0.084	0.126	0.163	0.206	0.212	0.092	-0.005	0.076	0.015	0.028	0.065	0.213	0.273	0.082	0.196
O-PP-Review Oper Perf	-0.017	0.367	0.025	-0.005	0.086	0.108	0.325	0.168	0.319	0.117	-0.031	0.041	0.115	-0.025	0.112	0.261	0.13	0.162	0.051	0.277
O-PP-Info Protect Controls	0.031	0.558	0.112	0.002	0.008	0.229	0.217	0.199	0.194	0.119	0.018	-0.003	-0.069	0.017	0.072	0.054	0.325	0.265	0.148	0.057
O-PP-Communic Policy	0.021	0.33	0.041	0.012	0.116	0.235	0.167	0.306	0.314	0.173	-0.002	0.092	0.128	0.002	0.018	0.319	0.293	0.138	0.019	0.232
O-PP-Monitoring Int Controls	0.213	0.392	0.112	0.205	0.069	0.186	0.035	0.448	0.13	0.292	0.146	0.062	0.088	0.093	0.042	0.116	0.267	0.14	0.035	0.178
O-PP-Misreposting Controls	0.309	0.475	0.112	-0.038	0.191	0.155	0.073	0.349	0.051	0.158	0.052	0.043	0.161	0.156	0.075	0.023	0.01	0.277	0.255	0.073
O-PP-Fraud Controls	0.234	0.465	0.283	0.053	0.058	0.156	0.042	0.263	0.096	0.225	0.038	0.008	0.087	0.073	0.09	0.065	0.135	0.098	0.22	0.214
O-TF-Facilities	0.077	0.122	-0.013	-0.105	-0.17	0.253	0.037	0.142	0.354	0.09	0.098	0.144	0.218	0.068	0.162	0.012	0.153	0.5	0.065	0.041
O-TF-Proc Technologies	0.07	0.116	0.299	0.123	0.125	0.007	0.245	0.009	0.068	0.123	0.153	0.007	0.029	0.061	0.159	-0.024	0.105	0.658	0.061	0.229
O-TF-Info Tech	-0.106	0.011	0.298	0.161	0.073	0.061	0.419	0.247	0.073	0.2	0.134	0.019	-0.062	0.105	0.105	-0.021	0.135	0.182	-0.056	0.422
O-TF-Obsolescence	-0.094	0.022	0.253	-0.003	0.118	0.094	0.222	0.213	0.059	0.134	0.149	0.208	0.03	0.054	0.137	0.074	0.094	0.541	0.08	0.362
O-TF-Controls integr	0.098	0.159	0.065	0.038	0.013	0.089	0.174	0.593	0.218	0.069	0.279	0.072	0	0.028	0.151	0.049	0.227	0.218	0.123	0.291
O-TF-Quality Assurance	0.12	0.145	0.183	0.055	0.145	0.08	0.258	0.658	0.133	0.129	0.039	0.065	0.006	0.076	0.096	-0.038	0.28	0.207	0.082	0.195
O-CS-Cust Intimacy	0.096	0.244	0.156	0.207	0.167	0.063	-0.101	0.065	0.566	-0.109	-0.017	0.096	0.04	0.226	-0.05	-0.013	0.012	0.196	0.233	0.176
O-CS-Supp Intimacy	0.064	0.096	-0.039	0.061	0.154	-0.039	0.043	0.057	0.726	0.238	0.208	0.062	-0.034	0.048	0.116	0.184	0.011	0.157	0.195	0.015
O-CS-Sourcing	0.175	0.123	-0.111	0.17	0.264	-0.029	0.135	0.266	0.626	0.227	0.144	0.067	0.024	0.004	0.141	-0.029	0.256	0.03	-0.01	0.036
O-CS-Contracts	-0.037	0.01	0.141	0.085	0.183	0.148	0.165	0.203	0.289	0.3	-0.064	0.134	0.213	-0.003	0.069	0.127	0.466	0.057	0.029	0.188
O-CS-Prod Failure	0.082	0.172	0.089	0.204	0.279	0.099	0.218	0.384	0.375	0.277	0.087	-0.042	-0.001	0.22	0.103	-0.044	0.061	0.089	0.196	0.072
O-EX-Regulatory Compliance	0.174	0.11	0.045	-0.039	0.013	0.243	0.204	0.132	-0.061	0.111	0.316	0.199	0.084	0.007	0.038	0.005	0.612	0.18	0.19	0.134
F-HR-Board	-0.071	0.027	0.052	-0.033	0.038	0.042	0.048	0.021	0.029	-0.033	0.176	0.046	0.081	0.839	0.075	0.038	0.11	-0.098	0.001	0.2
F-HR-Committees	-0.042	0.137	-0.002	0.24	0.065	0.77	0.04	0.078	0.019	-0.055	0.039	0.105	0.006	0.232	0.177	-0.049	0.096	-0.123	-0.002	0.154
F-HR-Executives	-0.129	0.219	0.269	0.041	0.048	0.03	0.143	0.095	-0.097	-0.035	0.12	0.258	0.41	0.286	0.197	0.036	0.36	-0.12	0.14	0.126
F-HR-Seniors	0.066	0.093	0.071	0.243	0.156	0.263	-0.089	0.362	0.026	0.178	-0.04	0.614	0.095	-0.123	0.012	0.055	0.033	0.1	0.141	-0.132
F-HR-RiskPers	0.065	0.038	0.034	0.7	-0.021	0.328	-0.058	0.181	0.163	0.017	0.111	0.232	0.019	-0.031	0.117	0.097	-0.014	0.068	0.082	0.182
F-PP-Finance Risk	0.004	0.003	-0.021	0.198	0.222	-0.038	0.218	0.126	0.088	-0.084	0.495	-0.027	0.193	0.052	0.102	0.244	0.039	0.45	0.107	0.106
F-PP-Liquidity Risk	0.01	0.105	0	0.079	0.222	0.019	0.303	0.114	0.16	-0.054	0.671	-0.062	0.017	0.143	0.156	0.026	0.114	0.239	0.013	0.004
F-PP-Cash Flow Risk	-0.03	0.044	0.08	0.038	0.277	-0.061	0.586	0.019	0.099	-0.154	0.338	-0.137	0.322	0.009	0.235	0.13	0.095	0.127	0.131	0.043
F-PP-Cust Credit Risk	-0.013	0.231	0.257	-0.017	0.499	0.096	0.018	0.133	0.102	0.191	0.266	-0.071	0.189	0.024	0.049	0.112	-0.017	0.141	0.222	0.196
F-PP-Supp Credit Risk	0.07	0.066	0.165	0.024	0.644	0.078	0.007	0.027	0.177	0.257	0.27	0.097	0.16	0.015	0.209	0.112	-0.013	0.128	0.159	0.029
F-PP-Partner Credit Risk	0.062	0.144	0.309	0.218	0.377	0.023	-0.125	0.098	0.135	0.233	0.528	0.089	0.064	0.094	0.076	0.086	0.013	0.098	0.053	0.052
F-PP-Equity Risk	0.085	-0.027	0.127	0.05	0.183	-0.02	0.002	0.046	0.075	0.096	0.553	-0.056	0.077	0.023	0.474	0.15	0.081	-0.032	0.041	-0.048
F-PP-Interest Rates	0.019	-0.047	0.082	-0.014	0.035	0.08	-0.051	0.028	0.018	0.03	0.463	0.073	0.06	0.208	0.618	0.116	0.152	0.048	0.121	0.024
F-PP-Exchange Rates	0.107	0.027	-0.025	0.034	0.054	0.206	0.056	0.026	0.079	0.051	0.017	-0.027	0.006	0.118	0.819	0.059	-0.05	0.225	0.061	0.144
F-PP-Commodity Prices	0.049	0.034	0.156	0.149	0.283	0.007	-0.002	0.099	0.015	0.043	0.031	0.137	0.155	0.154	0.639	0.279	0.118	0.148	0.039	0.024
F-TF-Tech Infra	0.153	0.116	0.685	0.028	0.033	-0.028	0.337	-0.081	0.013	0.063	0.064	0.23	0.127	0.126	0.108	0.068	0.254	0.193	0.01	0.083
F-TF-Info Infra	0.12	0.087	0.751	0.024	0.114	-0.047	0.323	0.09	-0.092	0.092	0.008	0.172	0.079	0.14	0.093	0.055	0.155	0.15	-0.041	0.138
F-TF-Know Infra	0.165	0.143	0.684	0.04	0.211	0.125	0.142	0.225	-0.051	0.023	0.115	0.062	0.179	-0.016	0.03	-0.003	0.068	0.153	0.064	0.027
F-TF-Repost tools	0.191	0.082	0.673	0.101	0.065	0.142	0.076	0.192	0.232	0.085	0.156	0.012	0.059	-0.025	0.14	0.126	0.019	0.162	0.165	0.091
F-CS-Customer Loss	0.089	0.056	0.079	0.045	0.558	0.029	-0.053	-0.048	0.049	0.049	0.275	-0.03	-0.053	-0.008	0.082	0.203	0.223	0.03	0.29	0.371
F-CS-Supplier Quality	-0.062	-0.049	0.082	-0.076	0.643	-0.066	0.055	0.215	0.267	0.088	0.08	0.084	0.037	0.075	0.272	0.133	0.155	0.167	0.247	0.126
F-CS-Supply disrupt	0.13	-0.031	0.011	0.109	0.603	0.007	0.139	0.153	0.308	0.111	0.2	0.083	-0.006	0.094	0.305	0.106	0.131	0.08	0.209	0.113
F-EX-Regulatory Change	0.3	0.139	0.143	-0.056	0.079	0.179	0.11	-0.053	0.194	-0.107	0.315	0.053	0.047	-0.137	0.205	0.076	0.364	0.159	0.171	0.311
H-HR-Board	0.121	-0.133	0.003	0.11	0.013	-0.038	0.087	0.011	0.089	0.036	0.109	0	0.03	0.4	0.199	0.719	-0.082	0.118	0.108	-0.032
H-HR-Committees	0.089	0.053	-0.052	0.241	0.121	0.362	-0.015	0.013	0.008	0.031	0.12	-0.033	0.005	0.106	0.095	0.717	0.056	0.035	0.028	0.055
H-HR-Executives	0.087	0.151	0.119	0.081	0.083	-0.119	0.059	-0.074	0	0.039	0.028	0.178	0.346	0.044	0.11	0.702	0.131	-0.097	0.125	0.167
H-HR-Seniors	0.095	0.311	-0.088	0.176	-0.079	0.037	0.054	0.125	0.071	0.211	-0.058	0.411	0.04	-0.154	0.194	0.217	-0.03	-0.128	0.384	-0.077
H-HR-RiskPers	0.209	0.099	0.003	0.741	0.032	0.099	0.16	0.022	0.027	0.114	-0.019	0.175	-0.005	-0.013	0.15	0.22	-0.039	0.017	0.111	-0.059
H-PP-Bus Cont	0.73	0.151	0.128	0.1	0.128	0.043	0.045	0.12	0.114	0.046	0.041	-0.025	0.172	0.116	0.219	0.224	0.143	0.176	0.067	0.074
H-PP-Disaster Resp	0.73	0.14	0.173	0.138	-0.007	0.067	-0.02	0.127	0.185	0.011	0.083	0.038	0.171	0.049	0.11	0.17	0.217	0.165	0.075	0.091
H-PP-Reporting	0.58	0.143	0.129	0.207	0.077	0.179	0.11	0.19	0.172	0.151	0.041	0.118	0.083	0.063	-0.06	0.19	0.205	0.109	0.079	0.088
H-TF-Facilities	0.65	-0.01	0.275	0.121	0.055	0.142	0.172	0.099	0.002	0.106	0.074	-0.005	0.048	0.016	0.168	0.136	0.187	0.068	0.163	0.08
H-TF-Plans	0.62	0.108	0.225	0.128	-0.036	0.218	0.065	0.205	0.19	0.017	0.147	0.074	0.106	0.067	0.14	0.206	0.187	0.014	0.058	0.18
H-CS-Customer	0.62	0.111	0.076	0.204	0.36	0.09	0.021	0.068	0.129	0.045	0.145	0.166	-0.089	0.161	0.209	0.019	-0.05	0.026	0.106	0.166
H-CS-Supplier Disrupt	0.53	0.073	0.021	0.174	-0.453	0.079	0.117	0.195	0.162	0.084	0.164	0.066	0.036	0.11	0.232	0.136	-0.069	0.057	0.194	0.116
H-EX-Regulatory Change	0.46	0.014	0.12	0.18	-0.007	0.036	0.083	0.054	0.036	0.178	0.37	0.111	-0.006	-0.04	0.038	0.204	0.175	0.069	0.345	0.172

incipal Component Analysis.
ocwith Kaiser Normalization.
n converged in 68 iterations.

Figure 10.
Principal component analysis

firm attributes, information, knowledge, etc. controlled by a firm" not only enable the firm to conceive of and implement strategies that improve its efficiency and effectiveness, they are also the ones that create risk exposure. This exposure needs to be addressed, and our framework constitutes a dynamic capability (Eisenhardt and Martin, 2000), or an organizational and strategic routine, by which firms achieve new resource configurations as markets change. As far as we know, we are the first to link the various classes of risks to an extended set of organizational resources, based on resource-based theory, and arguing for this framework as a key to creating new dynamic capabilities. The interaction points between the sets of resources and risk classes are identified to be the *locus* around which the risk exposure needs to be assessed. Our research contributions have been in grounding a new framework in existing theory and validating the framework on a set of highly skilled professionals by executing a well-crafted survey pilot tested and approved by the American Institute of Certified Public Accountants (AICPA). The survey subjects were recruited from the membership database of the AICPS, focusing primarily on CFOs. The survey yielded a data set of 227 valid responses that was used to validate the framework, thereby bridging the gap between practice and theory.

The proposed linking of the risk classes to resource-based theory and dynamic capability development is a major contribution to research, as it offers a new lens that provides guidance to risk identification. But, there is no doubt that our theoretically grounded framework serves only as a starting point to measuring the impacts of use of the framework. More research is needed to study the operational or behavioral effectiveness related to the differences between not using this framework and using it (or alternative frameworks, once proposed).

In practice, determining and effectively managing risks at enterprise level is a dynamic process that results in proper assessment of the firm's risk profile at a particular time. Given the complex nature of the modern-day organization and rapidly changing internal and external environments, it is important that managers are proactive in identifying and managing risks. Our framework is perceived by experts as being a useful tool. It allows managers to identify risks based on 20 interaction sets emanating from four major risk classes and five different resource categories. Our survey data validate the fact that managers find our framework valuable for risk identification and management. Within an organization, as a starting point, managers could use these 20 interaction sets to identify detailed list of resources under each category that are exposed to various risk classes and their possible interdependence. Note that the number of resources under each category will depend of the granularity at which these resources are defined and are idiosyncratic to individual organizations. These 20 interaction sets should be thought of as a guide for the management to think about risk expansively and help identify risks that are specifically material to the organization. Risk exposure is not a snapshot event in an organization's time horizon. Rather, risk identification is an ongoing process, and our framework allows organizations to handle increasing complex risks and/or identifying them based on how the organizational resources may be exposed over time. Managers could use a form of risk control analytics (monitoring dashboard of all identified risks under each interaction sets on a regular basis) to become more proactive in managing risk or exploiting opportunities across an enterprise. It is our understanding that positive return on investment on the implementations of these tools would encourage managers to embrace them at the enterprise level, and our model could be used incrementally, in part by part, to achieve such goals. This approach could promote and enhance risk transparency at the enterprise level, both in terms of risk reporting and external public disclosure. As a starting point, survey executed in this

paper validates the usefulness of this framework from the CFO perspective, which should serve as a strong indication of implications for practice and society. We also argue that the proposed method is generally applicable and has significant contributions to practice in terms of risk identification and risk management.

Like any other framework, our proposed model does have limitations that predominantly exist from the fact that human judgment in decision-making is not always data-driven, and hence, a proper risk exposure could be ignored based on pure arguments of cost and benefits from domain experts. Under given circumstances, management can always overwrite a model-based decision. However, we argue that our framework promotes thorough risk identification, and therefore may enable a more inclusive analysis of risks. Further research is needed to considering second-order interactions within the risk classes. A strong, standard model is key for academics and organizations to study and manage risk. Building on the current practice and research, this paper outlined a framework for risk identification and risk management that may promote broader thinking about risk identification and management. Without linking the individual organizational resources to risk via interaction points, it could be very hard to identify risks like the one demonstrated by the 2015 emissions issues for Volkswagen's diesel engines.

Note

1. For case summary and additional references, available at: https://en.wikipedia.org/wiki/2008_Soci%C3%A9t%C3%A9_G%C3%A9n%C3%A9rale_trading_loss

References

Alviniussen, A. and Jankensgard, H. (2009), "Enterprise risk budgeting – bringing risk management into the financial planning process", *Journal of Applied Finance*, Vol. 19 Nos 1/2.

Amit, R. and Schoemaker, P.J.H. (1993), "Strategic assets and organizational rent", *Strategic Management Journal*, Vol. 14 No. 1, pp. 33-46.

Arena, M., Arnaboldi, M. and Azzone, G. (2010), "The organizational dynamics of enterprise risk management", *Accounting, Organizations and Society*, Vol. 35 No. 7, pp. 659-675.

Barney, J. (1991), "Firm resources and sustained competitive advantage", *Journal of Management*, Vol. 17 No. 1, pp. 99-120.

Barney, J. and Hesterly, W.S. (2006), *Strategic Management and Competitive Advantage*, Pearson Prentice Hall, Upper Saddle River, NJ.

Beasley, M. Bradford, M. and Pagach, D. (2004), "Outsourcing? At your own risk: before outsourcing any process or function, it's essential to assess the risks enterprise-wide", Strategic Finance, pp. 22-29.

Beasley, M.S. Branson, B. and Hancock, B. (2011), "Developing key risk indicators to strengthen enterprise risk management", Published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), New York, NY, January.

Beasley, M.S., Pagach, D. and Warr, R. (2008), "Information conveyed in hiring announcements of senior executives overseeing enterprise-wide risk management processes", *Journal of Accounting, Auditing and Finance*, Vol. 23 No. 3, pp. 311-332.

COSO (2004), "Enterprise risk management – integrated framework", Committee of Sponsoring Organizations of the Treadway Commission.

COSO (2016), "Enterprise risk management–aligning risk with strategy and performance", Public Exposure Draft.

Cepeda, G. and Vera, D. (2007), "Dynamic capabilities and operational capabilities: a knowledge perspective", *Journal of Business Research*, Vol. 60 No. 5, pp. 426-437.

Drew, S.A., Kelley, P.C. and Kendrick, T. (2006), "CLASS: five elements of corporate governance to manage strategic risk", *Business Horizons*, Vol. 49 No. 2, pp. 127-138.

Eisenhardt, K.M. and Martin, J.A. (2000), "Dynamic capabilities: what are they?", *Strategic Management Journal*, Vol. 21 Nos 10/11, pp. 1105-1121.

Gates, S. (2006), "Incorporating strategic risk into enterprise risk management: a survey of current corporate practice", *Journal of Applied Corporate Finance*, Vol. 18 No. 4, pp. 81-90.

Gordon, L.A., Loeb, M.A. and Tseng, C.Y. (2009), "Enterprise risk management and firm performance: a contingency perspective", *Journal of Accounting and Public Policy*, Vol. 28 No. 4, pp. 301-327.

Kimbrough, R.L. and Componation, P.J. (2009), "The relationship between organizational culture and enterprise risk management", *Engineering Management Journal*, Vol. 21 No. 2, pp. 18-26.

Lam, J. (2014), "Enterprise risk management: from incentives to controls", Wiley Finance Series.

McNeil, A.J., Frey, R. and Embrechts, P. (2015), *Quantitative Risk Management: Concepts, Techniques and Tools*, Princeton University Press, Princeton, NJ.

Mathews, J.A. (2003), "Competitive dynamics and economic learning: an extended resource-based view", *Industrial and Corporate Change*, Vol. 12 No. 1, pp. 115-145.

Mishra, B. and Rolland, E. (2009), "A strategic framework for city marketing: the SSRM", in Gasco-Hernandez, M. and Torres-Coronas, T. (Eds), *Information Communication Technologies and City Marketing: Digital Opportunities for Cities around the World*, Information Science Ref, Hershey, PA.

Olson, D.L. and Dash Wu, D. (2010), "A review of enterprise risk management in supply chain", *Kybernetes*, Vol. 39 No. 5, pp. 694-706.

Rolland, E., Patterson, R. and Ward, K.F. (2009), "Dynamic capabilities and e-Service", *Canadian Journal of Administrative Sciences/Revue Canadienne Des Sciences de L'administration*, Vol. 26 No. 4, pp. 301-315.

Shad, M.K. and Lai, F.W. (2015), "A conceptual framework for enterprise risk management performance measure through economic value added", *Global Business and Management Research: An International Journal*, Vol. 7 No. 2.

Shah, J. (2009), "Supply chain risk management: academic perspective", *IIMB Management Review*, Vol. 21 No. 2, pp. 149-157.

Smithson, C. and Simkins, B.J. (2005), "Does risk management add value? A survey of the evidence", *Journal of Applied Corporate Finance*, Vol. 17 No. 3, pp. 8-17.

Weitzner, D. and Darroch, J. (2010), "The limits of strategic rationality: ethics, Enterprise risk management, and governance", *Journal of Business Ethics*, Vol. 19 No. 3, pp. 361-372.

Further reading

Beasley, M.S., Clune, R. and Hermanson, D.R. (2005), "Enterprise risk management: an empirical analysis of factors associated with the extent of implementation", *The Journal of Accounting and Public Policy*, Vol. 24 No. 6, pp. 521-531.

ISO (2015), "ISO 31000: risk management – A practical guide for SMEs", ISO, Vernier.

von Kanel, J., Cope, E.W., Deleris, L.A. and Nayak, N. (2010), "Three key enablers to successful enterprise risk management", *IBM Journal of Research and Development*, Vol. 54 No. 3.

Appendix 1

Survey Questions & Responses

SA: Strongly Agree
A: Agree
Neutral: No Opinion
D: Disagree
SD: Strongly Disagree

INTERACTIONS	SURVEY REPONSES		
A: Strategic Risk | Personnel & Structure	**SA + A**	**Neutral**	**D + SD**
The following personnel are actively engaged in strategic risk management:			
a) Board of Directors	27% + 45%	19%	8% + 1%
b) Committees or Specialty Groups (such as an Audit-, Budget-, Risk-, and Corporate Governance Committee)	29% + 35%	28%	6% + 2%
c) Executive Management (Chairman, President, General counsel, partners, CxO - such as CEO, CFO, CRO, CIO, COO, ...)	70% + 28%	1%	0% + 0%
d) Senior Managers & Managers (Line, operational, plant, business continuity, and other managers)	28% + 50%	14%	6% + 1%
e) Risk Professionals (such as risk, statistical, and actuarial experts)	24% + 25%	6%	4% + 4%
B. Strategic Risk | Process and Plans			
The organization provides:			
a) An appropriate governance structure for enterprise risk management	23% + 53%	14%	8% + 2%
b) A suitable incentive system for top management to actively engage in enterprise risk management	10% + 31%	31%	24% + 4%
c) An effective control environment (the control environment serves as the foundation for the internal control activities)	21% + 60%	10%	7% + 1%
Strategic risk is managed by designing an effective control environment that considers:			
a) Employee attributes (such as integrity, ethics, and competence)	38% + 50%	7%	4% + 1%
b) Management attributes (the way management assign authority and responsibility, and in the organization and development of employees)	35% + 53%	8%	4% + 1%
C. Strategic Risk | Facilities and Operational Assets (Technologies)			
The organization has the appropriate operational assets (technologies & facilities) for managing strategic			
a) Technology infrastructure (hardware, software, networks)	23% + 54%	12%	12% + 1%
b) Information infrastructure (relevant data, databases)	17% + 54%	18%	10% + 1%
c) Knowledge infrastructure (models for analyzing enterprise risk data)	11% + 39%	26%	22% + 2%
d) Risk reporting tools/dashboards/indicators	10% + 39%	23%	25% + 3%
D. Strategic Risk | Customers & Suppliers			
The organization manages strategic risks associated with Supply chain disruptions/failure	13% + 48%	30%	9% + 0%

(*continued*)

E. Strategic Risk | External

The organization manages strategic risks associated with Community, state, federal, or international regulations (including regulatory agencies like FDA, OSHA, EPA)	23% + 50%	19%	8% + 1%

INTERACTIONS	SURVEY REPONSES		
A: Operational Risk | Personnel & Structure	**SA + A**	**Neutral**	**D + SD**
The following personnel are actively engaged in operational risk management:			
a) Board of Directors	25% + 44%	21%	10% + 1%
b) Committees or Specialty Groups (such as an Audit-Budget-, Risk-, and Corporate Governance Committee)	28% + 34%	28%	8% + 2%
c) Executive Management (Chairman, President, General counsel, partners, CxO-such as CEO, CFO, CRO, CIO, COO, ...)	56% + 41%	2%	1%
d) Senior Managers & Managers (Line, operational, plant, business continuity, and other managers)	28% + 59%	10%	4% + 1%
e. Risk Professionals (such as risk, statistical, and actuarial experts)	18% + 29%	41%	6% + 5%
B: Operational Risks | Process and Plans			
Operational risk is managed by designing an effective internal control environment that considers:			
a) Employee attributes (such as integrity, ethics, and competence)	36% + 56%	5%	3% + 0%
b) Management attributes (the way management assign authority and responsibility, and in the organization and development of employees)	38% + 54%	6%	2% + 0%
c) Comprehensive risk factors that impact the enterprise	24% + 61%	12%	4% + 0%
The following issues are considered in the design of control activities:			
a) Clear segregation of duty	42% + 51%	6%	1% + 1%
b) Proper procedures for approvals, authorization, verifications, and reconciliation (such as implementation of controls procedures in transaction cycles)	44% + 51%	3%	2% + 1%
c) Proper safeguard of assets	41% + 55%	3%	1% + 1%
d) Review of operating performance	46% + 39%	12%	4% + 0%
e) Incorporate information protection controls (such as IT security, privacy, appropriate information access)	47% + 42%	8%	3% + 1%
f) Policies and procedures for effective communication of information within and across the organization	24% + 54%	15%	6% + 1%
g) Effective monitoring of internal control systems	27% + 57%	13%	3% + 1%
h) Controls against financial misreporting	37% + 56%	4%	2% + 1%
i) Controls against fraud	35% + 59%	4%	2% + 0%

(*continued*)

Appendix 2

C: Operational Risks | Facilities and Operational Assets (Technology)

The organization manages operational risks with respect to:			
a) Having suitable facilities (such as offices, production facilities, etc.)	27% + 59%	10%	4% + 1%
b) Having process technologies that are aligned with competitive strategy (such as the latest MRI scanner for a teaching hospital, vs. an x-ray machine for dentist)	20% + 57%	16%	7% + 1%
c) Having appropriate information technologies (such as enterprise resource planning, customer relationship management, and supply chain management systems)	20% + 55%	16%	9% + 0%
d) Obsolescence of technologies and facilities	12% + 48%	27%	13% + 1%
e) Systems controls integration	15% + 55%	21%	8% + 1%
f) Systems quality assurance	15% + 57%	20%	7% + 1%

D: Operational Risks | Customers & Suppliers

The organization manages operational risks related to:			
a) Customer interactions	30% + 59%	10%	1% + 1%
b) Supplier interactions	16% + 58%	24%	3% + 1%
c) Procurement & sourcing	17% + 61%	17%	4% + 0%
d) Contract compliance	23% + 57%	17%	3% + 0%
e) Product/service failures & liabilities	23% + 55%	18%	4% + 1%

E: Operational Risks | External

The organization manages the operational risks associated regulatory compliance (community, state, federal, and international regulations)	33% + 53%	10%	2.1% + 0.5%

INTERACTIONS	SURVEY REPONSES		
A: Financial Risks | Personnel & Structure	**SA + A**	**Neutral**	**D + SD**
The following personnel are actively engaged in financial risk management:			
a) Board of Directors	31% + 42%	19%	7% + 1%
b) Committees or Specialty Groups (such as an Audit-, Budget-, Risk-, and Corporate Governance Committee)	28% + 35%	29%	6% + 2%
c) Executive Management (Chairman, President, General counsel, partners, CxO such as CEO, CFO, CRO, CIO, COO, ...)	70% + 26%	3%	1% + 0%
d) Senior Managers & Managers (Line, operational, plant, business continuity, and other managers)and other managers)	31% + 52%	13%	6% + 5%
e) Risk Professionals (such as risk, statistical, and actuarial experts)	18% + 28%	43%	6% + 5%

(*continued*)

B: Financial Risks | Process & Plans

Operational processes enable the organization to manage the following financing/liquidity risks:			
a) Financing risk (ability to get projects financing on timely basis)	33% + 51%	12%	4% + 0%
b) Market liquidity risk (availability of liquid markets)	26% + 48%	20%	5% + 1%
c) Cash flow risk (ability to cover cash outflows when due)	43% + 49%	5%	3% + 1%

Operational processes enable the organization to manage the following credit risks (possibility of default of customer, or inability to meet a commitment by a supplier/partner)			
a) Customer credit risk	30% + 47%	16%	6% + 1%
b) Supplier credit risk	14% + 49%	28%	8% + 1%
c) Partner credit risk	12% + 41%	38%	8% + 2%

Operational processes enable the organization to manage the following market risks (possible losses due to changes in future market prices or rates):			
a) Equity risk	16% + 46%	29%	8% + 1%
b) Interest rates	22% + 45%	23%	9% + 1%
c) Exchange rates	8% + 22%	61%	8% + 2%
d) Commodity prices	11% + 27%	53%	9% + 0%

C: Financial Risks | Facilities and Operational Assets (Technologies)

The organization has the appropriate technology & information tools for managing financial risk:			
a) Technology infrastructure (hardware, software, networks)	28% + 52%	12%	7% + 0%
b) Information infrastructure (relevant data, databases)	25% + 56%	13%	7% + 0%
c) Knowledge infrastructure (models for analyzing financial risk data)	24% + 50%	14%	12% + 0%
d) Risk reporting tools/dashboards/indicators	18% + 41%	20%	18% + 2%

D: Financial Risks | Customers & Suppliers

The organization manages financial risk related to:			
a) Loss of major customer	22% + 47%	22%	9% + 0%
b) The quality of the suppliers' products/services	17% + 54%	20%	8% + 1%
c) Supply chain disruption/failure	12% + 49%	29%	9% + 1%

E: Financial Risks | External

The organization manages the financial risks associated with regulatory changes (community, state, federal, international -- for example, the SEC's recent ban of short-sales)	23% + 46%	26%	3.8% + 0%

(*continued*)

INTERACTIONS	SURVEY REPONSES		
A: Hazard Risks | Personnel and Structure	**SA + A**	**Neutral**	**D + SD**
The following personnel are actively engaged in hazard risk management:			
a) Board of Directors	12% + 31%	34%	18% + 4%
b) Committees or Specialty Groups (such as an Audit-, Budget-, Risk-, and Corporate Governance Committee)	15% + 32%	34%	17% + 2%
c) Executive Management (Chairman, President, General counsel, partners, CxO such as CEO, CFO, CRO, CIO, COO, ...)	37% + 44%	13%	4% + 1%
d) Senior Managers & Managers (Line, operational, plant, business continuity, and other managers)	25% + 49%	13%	4% + 1%
e) Risk Professionals (such as risk, statistical, and actuarial experts)	20% + 30%	37%	10% + 3%
B: Hazard Risks | Process & Plans			
Operational plans and processes:			
a) Address business continuity risks associated with hazards	24% + 60%	7%	8% + 1%
b) Address disaster response and recovery risks associated with hazards	25% + 53%	15%	7% + 1%
C: Hazard Risks | Facilities & Operational Assets (Technologies)			
Operational plans and processes:			
a) Generate hazard risk reports and indictors	11% + 32%	30%	23% + 4%
For managing hazard risk, the organization possesses:			
a) Appropriate technologies, facilities and operational assets	20% + 49%	19%	11% + 1%
D: Hazard Risks | Customers and Suppliers			
The organization manages hazard risk related to:			
a. Disruptions in delivery of products/services to their customers	17% + 56%	16%	10% + 1%
b. Supply chain/sourcing disruptions/failure	13% + 48%	28%	11% + 1%
E: Hazard Risks | External			
The organization manages potential risks arising from regulatory change related to hazards (such as building codes for earthquakes, or airline check-in procedures after 9/11)	12.8%+46.4%	30.70%	9.6% + 0.6%

About the authors

Birendra K. Mishra, PhD, is a Professor of Accounting and Information Systems at the UCR School of Business at the University of California, Riverside. He previously served as a faculty at the Arizona State University and the University of Texas, Dallas. His papers have appeared in such journals as *The Accounting Review*, *Management Science*, *Marketing Science*, *Information Systems Research* and others. His PhD is in Accounting from the University of Texas at Austin.

Erik Rolland, PhD, is a Professor and Dean of the College of Business Administration at California State Polytechnic University, Pomona, California. He has been a Professor at the University of California, Merced, the Anderson Graduate School of Management at the University of California, Riverside, the Fisher School of Business at the Ohio State University and has served as a Visiting Distinguished Professor with the Antai School of Management and Economics at the Shanghai Jiaotong University. His papers have appeared in journals such as *MIS Quarterly*, *Production and Operations Management*, *Operations Research*, *ACM Transactions on MIS*, *Decision Support Systems* and in numerous other journals. His PhD is in Business Administration from the Fisher College of Business, the Ohio State University. Erik Rolland is the corresponding author and can be contacted at: erolland@cpp.edu

Asish Satpathy, PhD, is a Lecturer in Information Systems at the UCR School of Business at the University of California, Riverside. He is a prolific educator and researchers, entrepreneur and technology product design consultant. His prior work includes developing and marketing innovative technology solutions and managing mission critical detector instrumentation and data analysis projects in Europe (CERN), Japan (KEK) and the USA (Stanford Linear Accelerator Center). He holds a PhD in experimental High Energy Physics from KEK Lab in Japan and an MBA from University of California, Irvine.

Michael Moore, PhD, C.P.A. is a Professor in Residence in the Department of Accounting at Loyola Marymount University, Los Angeles, CA. He previously served as an Accounting Professor at University of California, Riverside, University of Southern California, Colorado State University and the University of Texas, Austin. His papers have appeared in journals such as *The Accounting Review* and *Journal of Accounting Research*, as well as other accounting and tax journals. His PhD is from Pennsylvania State University.