Article

SAGE Open
October-December 2016: 1–17

DOI: 10.1177/2158244016680230
sgo.sagepub.com
SAGE

Research Insights About Risk Governance: Implications From a Review of ERM Research

Therese R. Viscelli[1], Mark S. Beasley[2], and Dana R. Hermanson[3]

Abstract

In recent years, expectations for increased risk governance have been placed explicitly on boards of directors. In response, boards are being held responsible for not only understanding and approving management's risk management processes, but they are also being held responsible for assessing the risks identified by those processes as part of overseeing management's pursuit of value. These increasing responsibilities have led a number of organizations to adopt enterprise risk management (ERM) as a holistic approach to risk management that extends beyond traditional silo-based risk management techniques. As boards, often through their audit committee, consider management's implementation of ERM as part of the board's risk oversight, a number of questions emerge that can be informed by academic research related to ERM. This article summarizes findings from ERM research to provide insights related to the board's risk governance responsibilities. We also identify a number of research questions that warrant further analysis by governance scholars. It is our hope that this article will spawn varying types of research about ERM and corporate governance.

Keywords

ERM, risk, risk management, corporate governance, audit committee, board of directors, internal audit

Introduction

In recent years, expectations have risen for effective risk oversight, especially during the recent financial crisis, and most of those expectations have been placed explicitly on the shoulders of boards of directors. Stock exchanges, regulators, legislators, credit rating agencies, and industry associations have implemented changes designed to strengthen enterprise-wide risk oversight with an emphasis on enhancing the board's role in risk governance (Dodd-Frank Act of 2010, 2010; National Association of Insurance Commissioners, 2013; New York Stock Exchange [NYSE], 2004; Securities and Exchange Commission [SEC], 2009; Standard & Poor's [S&P], 2012). Most of these place the onus of responsibility for owning risk governance on the board.

In terms of risk governance, there are two overarching responsibilities being placed on boards of directors:

1. The board of directors should understand and approve management's process for overseeing enterprise risks (i.e., the board assesses the enterprise risk management [ERM] process).
2. The board of directors should evaluate the risks identified by management's process for overseeing enterprise risks to govern the actions taken by management to create value (i.e., the board uses information from the ERM process).

Pressure to fulfill these responsibilities is causing many boards to place expectations on management to design and implement robust processes for identifying, assessing, managing, and monitoring the most significant enterprise-wide risks. In fact, almost 70% of over 1,000 executives surveyed indicate that many board members are asking for greater risk oversight involvement by senior management. That percentage grows to 88% for public companies (Beasley, Branson, & Hancock, 2015).

Often the board works through its audit committee to oversee management's risk management processes, and that results in the audit committee turning to executives in key accounting and financial reporting roles, such as the chief financial officer (CFO) or chief audit executive, for initial risk management leadership. Accordingly, the accounting profession has been actively involved in developing ERM methods. Specifically, Committee of Sponsoring Organizations of the Treadway

[1]Auburn University, AL, USA
[2]North Carolina State University, Raleigh, USA
[3]Kennesaw State University, GA, USA

Corresponding Author:
Dana R. Hermanson, Dinos Eminent Scholar Chair of Private Enterprise, School of Accountancy, Kennesaw State University, 560 Parliament Garden Way, Kennesaw, GA 30144-5591, USA.
Email: dhermans@kennesaw.edu

Commission (COSO; 2004) issued *Enterprise Risk Management—Integrated Framework* to provide directors and managers with a model of the ERM process.

In response to these emerging expectations, a number of organizations have adopted ERM to enhance the organization's enterprise-wide risk oversight. ERM is a way to coordinate all the risk management activities so that management and the board have a top-down, enterprise-wide view of the most important risks to the enterprise (COSO, 2004).

One of the challenges for the board of directors in fulfilling its risk governance responsibilities is determining whether or not management's ERM practices are designed and operating effectively. In most situations, the board of directors is heavily, if not solely, dependent on management's description and self-assessment of the effectiveness of their risk management processes. Boards may be unsure as to whether the ERM processes implemented by management are appropriate and consistent with emerging best practices, and they may question whether those processes generate risk information that the board and management can use to design and implement strategies to protect and enhance stakeholder value. In summary, boards are in need of information to help them fulfill their risk governance oversight responsibilities.

To respond to this need, we examine the emerging body of ERM-related research to provide insights relevant to board of director risk governance responsibilities. While the overall volume and extent of ERM research is relatively small, we review the emerging academic literature on ERM by performing several searches for articles that provide insights related to questions boards may have in regard to enterprise risk governance. Specifically, we summarize findings from ERM research that provides insights to the following questions related to the board's two primary risk governance responsibilities:

1. Research insights to inform the board as it assumes responsibility for understanding and approving management's risk management processes that address these questions:
    a. What types of organizations adopt ERM as a risk management paradigm?
    b. What techniques comprise an ERM process?
    c. What is the role of internal audit (IA) in ERM?
2. Research insights to inform the board as it assumes responsibility for evaluating risk information generated by ERM processes as it governs management's strategic actions to protect and enhance stakeholder value that address these questions:
    a. How are organizations integrating ERM processes with strategy?
    b. How does ERM affect firm value and performance?
    c. How does organizational culture affect the value of ERM?

We believe the emerging stream of academic research about ERM provides insights to boards as they assume responsibilities for risk governance. To synthesize that research for boards and other governance players, we summarize key insights by organizing our review of the key findings along the above questions. One of our goals is to synthesize this research to inform boards as they assume greater risk oversight responsibilities.

Because research on ERM is still emerging, we also believe there is significant opportunity for future research to provide additional analysis of a number of issues related to enterprise-wide risk management. Building on a model similar to Bromiley, McShane, Nair, and Rustambekov (2015), who reviewed ERM literature to promote research by management scholars, we review ERM research to develop a number of ERM-related questions to be examined by governance scholars (including those in accounting, auditing, and finance), which is a second goal of this study.

The remainder of the article is organized as follows. The next section summarizes our methodology for identifying ERM-related research, and the following section summarizes key findings from articles that provide insights to inform the board as it assumes responsibility for understanding and approving management's risk management processes. We also include calls for additional research to provide additional insights related to that responsibility. The subsequent section summarizes key findings from articles that provide insights to the board as it assumes responsibility for evaluating risk information generated by ERM processes as it governs management's strategic actions to protect and enhance stakeholder value. That section also includes identification of a number of additional research topics relevant to the board. Finally, we provide overall conclusions.

Methodology for Reviewing ERM Academic Literature

We conducted several searches for articles to include in this review, focusing mostly on topics related to ERM. Using the electronic databases EBSCO, ProQuest, Science Direct, and Google Scholar, we searched on "ERM," "risk," "enterprise," and "COSO." The search was limited primarily to articles published after 1999, as ERM emerged mostly in the 2000s. While some articles from financial and insurance journals are included in this review, overall, we have excluded most highly technical, industry-specific research that does not directly address ERM. The references in each of the articles selected for review were examined to identify additional articles that may not have been found in the search of the electronic databases. The focus was on published academic journal articles, but selected working papers have been included as well. Thus, we summarize the key findings from ERM-related research papers to provide insights relevant to the board's two overarching risk governance responsibilities (see Figure 1).

Board's Role in Assessing ERM	Board Evaluation of Risk Information	Future Research
• Characteristics of ERM Adopters	• Strategy and ERM	• Appendix A
• ERM Implementation	• ERM and Firm Value and Performance	• Appendix B
• Internal Audit and ERM	• Culture and ERM	

Figure 1. Overview of analysis.
Note. ERM = enterprise risk management.

Research Insights Related to Board's Role in Assessing Management's ERM Processes

As expectations for more effective board risk governance have emerged, boards are being held accountable for understanding and approving management's processes for managing enterprise-wide risks. For example, the NYSE's governance rules place explicit responsibilities on the audit committee of the board to "discuss management's risk management and risk assessment processes," and the SEC's proxy disclosure rules implemented in 2010 require public companies to include disclosures about the board's role in risk oversight in the annual proxy statement (NYSE, 2004; SEC, 2009).

As boards assume greater responsibility for governance of management's risk oversight processes, they face a number of questions relevant to their obtaining an understanding of and approving management's approach to enterprise-wide risk oversight:

a. What types of organizations adopt ERM as a risk management paradigm?
b. What techniques comprise an ERM process?
c. What is the role of IA in ERM?

We use these questions as a framework for organizing our understanding of insights from ERM-related research performed to date, and we build upon that to generate a number of research topics that governance scholars may consider for future examination. See Table 1 for a summary of the insights.

Organizational Characteristics of ERM Adopters

In light of limitations associated with traditional risk management, a number of organizations have begun to adopt ERM. The goal of ERM is to manage risks at an enterprise level to ensure that entity-wide risks to the organization have been assessed, rather than just one aspect of risk to the organization. As boards of directors respond to the increasing expectations for more effective board risk governance, many are placing pressure on senior executives to implement ERM. However, in making that decision, boards may question whether the implementation of ERM in their organization makes sense.

Colquitt, Hoyt, and Lee (1999) conducted one of the first studies on risk management as it applied to risk financing strategies, describing it as *Integrated Risk Management*. The authors surveyed 379 firms and found that the role of risk manager was growing in scope to integrate across the organization, beyond traditional financial risk management. Industry and firm size also were associated with a more integrated approach to risk management and affected the financial tools used to oversee risk.

Subsequent studies examine organizational factors and financial characteristics of entities that adopt ERM to understand factors that affect the embrace of ERM as a risk management paradigm. However, as firms do not usually announce when they are embarking on an ERM implementation, it can be difficult for researchers to determine who has implemented ERM. Some researchers have used announcements of appointments of individuals to serve as chief risk officer (CRO) or disclosures of ERM activities as proxies for ERM adoption, while others have surveyed companies to understand their stage of ERM adoption.

Using the announcement of a CRO as a signal of ERM implementation, Liebenberg and Hoyt (2003) found that firms announcing a CRO were among the largest in their industry and were primarily in the financial and energy industries. While they did not find significant differences in firms' ownership (institutional vs. individual shareholders), the study did show a relationship between higher leverage and a greater likelihood to announce a CRO appointment.

Pagach and Warr (2011) also used the announcement of a CRO as a signal of ERM adoption to provide additional analysis of firmwide factors that might explain an entity's ERM implementation. The study found that firms with higher levels of leverage and larger size (assets) were more likely to announce the appointment of a CRO, consistent with Liebenberg and Hoyt (2003). In addition, they found that more volatile operating cash flows and greater stock volatility were positively associated with the announcement of a CRO. Contrary to findings of Liebenberg and Hoyt, who did

Table 1. Summary of Research Insights.

Board's role in assessing ERM	Board evaluation of risk information
Characteristics of ERM adopters Certain firmwide characteristics, such as size and industry, and certain board and other governance characteristics may be important factors that explain the decision by an organization to adopt ERM; however, there are mixed results related to other organizational factors and financial characteristics of firms that may be associated with ERM implementations.	*Strategy and ERM* While ERM is envisioned to provide an organization the opportunity to manage risks to achieving its strategic objectives, the limited academic research suggests that the integration of ERM and strategy has not been fully achieved, and organizations are struggling to fully leverage the strategic benefits of ERM.
ERM implementation Only a few studies specifically address the use of ERM frameworks, and they tend to focus on the COSO framework. Organizations might rely to some extent on those frameworks, but they are not likely to have implemented significant aspects of them. Articles that present specific case studies of firms adopting ERM show that ERM implementation varies widely across firms, even in the same industry. There is no one way to implement ERM, and organizations have approached the launch of ERM in a number of different ways. The limited access to data about specific techniques and internal processes used by organizations as they implement ERM has limited the ability to conduct academic research about the effectiveness of those processes. There is limited knowledge about specific factors that may affect the effectiveness of any number of ERM processes.	*ERM and firm value and performance* Better firm performance and increases in shareholder value are often used as arguments to embrace ERM. There is some research that contains evidence that ERM provides value, which is measured in different ways across those studies. While there is a general theme that ERM is associated with enhanced firm value, a number of those studies are limited to the insurance industry.
Internal audit and ERM Internal auditors have facilitated a number of ERM implementations, and there are concerns about the potential compromising of IA's objectivity and independence when IA assumes responsibility for ERM implementation.	*Culture and ERM* Organizational culture has a significant impact on the decision to implement ERM and on the effectiveness of that implementation. Without sufficient support of ERM by the CEO or board of directors, organizations may struggle in their efforts to find strategic value in their ERM processes. Research about the role of culture in the context of ERM is limited.

Note. ERM = enterprise risk management; COSO = Committee of Sponsoring Organization; IA = internal audit.

not find a difference in ownership structure between ERM adopters and the control group, Pagach and Warr found that firms with a high percentage of shares owned by institutional investors were more likely to have announced a CRO appointment, consistent with institutions' desire for greater risk control. In a subsample of firms where CEO compensation could be determined, Pagach and Warr found that firms where CEO compensation was sensitive to stock volatility were more likely to have a CRO.

In a study of U.S. insurers with ERM initiatives found using a word search, Hoyt and Liebenberg (2011) found that firms that have ERM initiatives were larger in size (assets) and had more institutional ownership, consistent with Pagach and Warr (2011). They did not find any significant association between the extent of leverage, stock return volatility, or opaqueness and the presence of ERM, as had been found in some previous studies. In another study of U.S. insurers, Lin, Wen, and Yu (2012) performed a similar word search and found that firms that had implemented ERM had more reinsurance and had greater geographic diversification compared with firms that had not implemented ERM.

Lundqvist (2014a) examined the relationship between ERM and credit risk management for a sample of banking institutions. The author found that credit risk was reduced as the level of ERM quality increased. No significant relationship was found between ERM quality and credit rating when controlling for governance characteristics such as board independence, large ownership by a group, and corporate governance measured by Thompson Reuters ASSET4 environmental, social, and governance (ESG) content. The author explains this last finding by suggesting that the market perhaps values the risk management function itself, while the credit rating agencies focus on risk governance aspects.

Other studies have used different proxies for ERM implementation. Beasley, Clune, and Hermanson (2005) explored organizational factors and their relationship to the stage of ERM implementation, based on surveys completed by internal auditors. Like other studies that focus on the association of firm characteristics and ERM implementation, they found firm size (revenues) was positively related to the stage of ERM. In addition, the study found firms that had a CRO, more independent directors, or explicit ERM calls from the CEO

and CFO were more likely to be at a more advanced stage of ERM, suggesting that top management support for ERM is critical for ERM implementation. Firms that engaged a Big Four auditor were also found to be further along in ERM implementation than were firms using smaller auditing firms. Firms in the banking, education, and financial industries were at a more advanced stage of ERM implementation than other industries. Finally, the study found that U.S. firms were less advanced in ERM implementation stage than international firms.

Using a sample of 825 firms located in the Netherlands, Paape and Spekle (2012) used the stage of ERM implementation (based on an ordinal scale of 1 to 5 with 4 to 5 being adopters of ERM and 1 to 3 having traditional, silo approaches to risk) to examine firm characteristics of those with more advanced ERM. They found larger firms and firms in financial industries were further along in ERM stage, and stock ownership was not found to be significant, which is consistent with findings in Liebenberg and Hoyt (2003). Unlike some of the other studies focused on ERM implementation, they did not find a relationship between having a Big Four auditor and ERM development. The authors also found that publicly traded firms, firms with a CRO, and those with an audit committee were further along in ERM implementation.

Baxter, Bedard, Hoitash, and Yezegel (2013) used S&P ERM quality ratings for banking and insurance industry firms to investigate variations in firm characteristics in relation to ERM ratings. Their results showed that companies with higher ERM ratings were more complex, had greater financial resources, and had better corporate governance. They also found that higher risk firms had lower quality ratings, which they attributed to resource constraints limiting the investment in ERM.

Lundqvist (2015) surveyed 145 firms on two major Nordic stock exchanges across multiple industries and found that firms implementing ERM are larger, in line with Beasley et al. (2005), Liebenberg and Hoyt (2003), and Pagach and Warr (2011). As with Paape and Spekle (2012), having a Big Four auditor did not affect risk governance, and firms in the financial industry were marginally more advanced in ERM, consistent with previous studies (Beasley et al., 2005; Liebenberg & Hoyt, 2003). In addition, the quality of the ERM governance and the following year's extent of leverage were positively related, consistent with limiting the use of free cash available to well-monitored managers. Finally, unlike prior research, organizations with higher leverage were less likely to have embraced ERM.

With the passage of Sarbanes–Oxley Act of 2002 (SOX), external auditors and corporate boards were assigned specific responsibilities for risk assessments related to financial statements. Farrell (2003) and Roth (2006) argued that firms can leverage SOX Section 404's requirement that management and auditors attest to the state of internal control over financial reporting effectiveness to promote the evaluation of risk at an enterprise level. Arnold, Benford, Canada, Kuhn, and Sutton (2007) found in a study of four firms that all of the firms believed their ERM was made more effective by the effort to become SOX compliant, but it was an "unintended" consequence of the 404 compliance effort.

Many companies have either board-level or management-level committees that have responsibility for ERM implementation. Previous studies identified as a limitation the ability to identify these firms. Subramaniam, McManus, and Zhang (2009) used the presence of a Risk Management Committee (RMC), as disclosed in a firm's annual report, to signal ERM implementation in 200 of the top 300 Australian Stock Exchange listed companies. Unlike some previous studies, they did not find a significant relation between ERM adoption and financial industry, board independence, or leverage. The authors did find that an independent board chair and larger boards were positively related to the presence of an RMC, as was organizational complexity as measured by the number of firm segments. Like Paape and Spekle (2012), having a Big Four auditor was not related to having an RMC.

Hines and Peters (2015) found that firms within the financial industry that formed an RMC had higher leverage (unlike Subramaniam et al., 2009); had a larger, more independent board; and were more likely to have a Big Four auditor. The authors also found that lower financial quality, international banking activity, and merger and acquisition activity where related to having an RMC.

Key implications for boards. Our analysis of ERM research to address our first question of interest (*What types of organizations adopt ERM as a risk management paradigm?*) reveals that that certain firmwide characteristics, such as size and industry, and certain governance characteristics may be important factors that explain the decision by an organization to adopt ERM. In particular, most studies find that larger firms and firms in certain regulated industries, particularly financial services and insurance, are associated with ERM adoptions. We also observe in some studies that certain governance factors, such as the level of board engagement, independence, and the presence of institutional investors, are also associated with ERM adoptions. Other factors, such as leverage, stock price or cash flow volatility, and the presence of a Big Four auditor are sometimes associated with a firm's decision to implement ERM. We summarize these insights in Table 1.

Opportunities for future research. The mixed results suggest the need for additional studies of the relationship of organizational factors and firm-level financial characteristics with ERM initiatives. There are a number of research questions related to firm- or industry-level characteristics that might affect a firm's decision to implement ERM that warrant further analysis. Column A of Appendix A includes a summary of these research questions.

ERM Implementation Process

While boards of directors and senior executives may conceptually embrace ERM, they often face a number of questions related to *how* organizations are implementing ERM to ensure its effectiveness in risk oversight. Because ERM is a relatively recent business paradigm, organizational leaders, including the board, have been calling for insights to help them understand specific processes that are needed when implementing ERM. A number of practitioner articles have been published with insights and suggestions related to processes important when implementing ERM. Some articles provide detailed steps, activities, and tools that should be used, while others describe individual firms that have implemented ERM, but not necessarily how they did it.

A number of ERM frameworks have been developed over the last decade to assist organizations in their design and implementation of ERM (COSO, 2004; International Organization for Standardization [ISO], 2009). When a board and its senior management team decide to implement ERM, they may seek conceptual frameworks related to ERM to guide the design of their ERM processes. In doing so, they may question what frameworks exist and which framework(s) are embraced by other organizations. Although only a few studies specifically address the use of ERM frameworks, we examine that research to summarize insights related to ERM conceptual frameworks.

In light of the prominence of COSO as a thought leader in ERM, Hayne and Free (2014) sought to understand the rise of the COSO framework to its point of prominence in risk management. The authors describe the processes and mechanisms used by COSO to create the COSO ERM framework and enable it to become so dominant. Through a series of interviews with key stakeholders in risk management and analysis of secondary documentation, the authors describe the creation of "hybrid" professional groups and the impact of these groups on the eventual adoption of the framework.

Tekathen and Dechow (2013) studied a German organization while it implemented ERM by using semi-structured interviews to understand how the organization implemented ERM. Because the organization professed to having used the COSO ERM framework, the authors compared the insights from the interviews with the COSO ERM framework to determine a fit to the framework. The authors stated that the COSO framework was based on "radical assumptions," and they asserted that the COSO framework implies that experts, expertise, and eventualities are aligned within an organization. The authors did not find this alignment in practice and concluded that ERM is not effective in reducing uncertainty, but instead increases the organization's interaction with uncertainty, unless processes are designed to support the alignment.

Paape and Spekle (2012) addressed the actual use of an ERM framework, in particular the COSO ERM framework, by 825 firms based in the Netherlands. The authors reported that 43% of the firms indicated they used the COSO framework, but the study only dichotomously captured the use of the framework (i.e., framework used or not used) and did not provide any detail as to how much or how the framework was used.

Beyond studying the use of ERM frameworks, the ability to conduct rigorous academic research about ERM implementation processes has been significantly limited by the lack of publicly available data about specific internal tools and techniques used as part of the risk oversight process. To address this limitation, studies that have focused on specific techniques used by firms when implementing ERM typically have used a case study approach or surveys to examine internal activities that are associated with ERM implementations.

Articles that present specific case studies of firms adopting ERM show that ERM implementation varies widely across firms, even in the same industry.[1] Arena, Arnaboldi, and Azzone (2010) studied three non-financial Italian firms over a 7-year period. All three firms professed to have an enterprise-wide risk management process, but each firm's approach and resulting ERM process was influenced by the firm's risk rationale. One firm's rationale for ERM was for compliance, the second firm's rationale was for stronger corporate governance to provide external assurance, and the third firm's rationale was to improve performance that would lead to enhanced company value. In another study, Arena, Arnaboldi, and Azzone (2011), again studied non-financial firms to understand the extent of ERM use and the relationship of ERM use to the characteristics of the ERM tools implemented. The authors found that firms that used ERM for proactive actions, such as planning at the strategic level, had ERM tools that were highly integrated through the organization at all levels and risk was centrally managed. The study also found that the role played by the ERM coordinator must include interaction with managers at all levels to help those managers understand the value of ERM and to encourage open discussions across functional areas of the risks.

A working paper by Mikes and Kaplan (2014) used contingency theory to identify design parameters that can explain variation in how three different case study organizations implemented ERM. Using interviews over the period of 2008-2012, they studied the implementation of ERM in detail at the three organizations. They classify the implementation into three fundamental risk management components and then classify the types of risks each firm encountered into three categories.[2] The authors found that organizations approached risk management in different ways, and the authors ultimately proposed that risk management is contingent on the organization's nature and ability to control different types of risks, which supports the view that risk management is different for each firm.

In a single-organization study, Aabo, Fraser, and Simkins (2005) studied ERM implementation at a Canadian electric company. They chronicle the process beginning with the creation of a CRO position. The authors describe the actual process including the techniques and tools that were used by the firm. The successful implementation of ERM integrated risk

into the workplace to the extent that the CRO position evolved into a low-maintenance position within the company.

Two articles examine the use of risk maps in the implementation of ERM. Woods (2009) performed a case study focused on a public sector entity's risk management control system to examine whether risk management systems are similar across large organizations by comparing the risk process with the Institute of Risk Management (IRM; 2002) model. Because the organization's process was easily mapped to the IRM model, the author argued that large organizations' overall risk processes are similar, as many organizations are following the IRM model. Woods also described the use of heat maps (risk maps) to rank the organization's risks on a scale from tolerable to material to severe (traffic light), which determines the level of control and monitoring (the resulting level of control and monitoring is the risk control system for the organization). The author concluded that the control system was affected by government policy, technology, and organization size.

Jordan, Jørgensen, and Mitterhofer (2013) examined the use of risk maps in the Norwegian petroleum industry as a way to represent risks within project management. They found that risk maps are being used to negotiate the boundaries of different project areas. The appearance of a risk object on a risk map resulted in it being more likely to be discussed. The risk maps were used to mediate concerns between groups and resulted in topics not shown being avoided, thus setting boundaries on the meeting discussions. Overall, the risk maps were used to create project identity, increase commitment to the project, and mediate between different groups in the company.

Studies that used surveys have each developed their own set of questions and surveyed a variety of groups, such as the American Institute of Certified Public Accountants (AICPA), The Conference Board, companies listed on the two Nordic stock exchanges, and firms based in the Netherlands. Paape and Spekle (2012) examined design choices of ERM by firms and the effects of the choices on risk management effectiveness. The authors found that the frequency of risk assessments and risk reporting and the use of quantitative approaches are associated with higher stages of ERM implementation. They also found that use of the COSO framework did not contribute to higher risk management effectiveness.

Another article based on the COSO ERM framework, Gates, Nicolas, and Walker (2012), surveyed Conference Board member firms to study the practical side of ERM.[3] Based on 150 completed responses, the authors modeled the direct impact that each of the components has on the subsequent component beginning with objective setting through performance. The study found that a structured approach to risk management can result in enhanced management and improved performance.

Beasley, Branson, and Pagach (2015) examined specific risk management processes associated with greater ERM maturity using a sample of 645 organizations across a number of industries. They found ERM maturity to be positively associated with boards of directors that are more actively engaged in risk oversight. ERM maturity also was positively related to organizations with risk management responsibilities assigned to a board committee, formal risk management reports to the board, and a formally articulated risk appetite.

Lundqvist (2014b) used survey results from 153 firms on two Nordic stock exchanges to understand ERM implementation and found four ERM implementation factors: (1) general internal environment and objective setting, (2) specific risk identification and risk assessment activities, (3) holistic organization of risk management, and (4) general control activities and information and communication. Lundqvist explained that Factors 1 and 4 could be viewed as "prerequisites" of an ERM implementation because they are necessary to support ERM but can exist without any effort toward risk management. Factor 2 represents efforts by the organization to manage certain types of risks, such as financial and compliance. Lundqvist identified Factor 3 as the true ERM identifier. Factor 3 represents organizational activities such as a formal, written risk appetite definition, senior management responsible for overseeing risk and risk management, and formal risk management reports provided to the board on a regular schedule. These activities are typical of firms approaching risk holistically the definition of ERM.

Ittner and Oyon's (2014) data consisted of responses from the corporate-level finance and risk executives of 1,051 international firms in multiple industries. The authors found that the breath of functional and hierarchical ownership of risk is positively associated with the sophistication of a firm's ERM implementation and that management practices are more closely associated with the levels and functions of the risk owners, not the number of owners. When the CFO of a firm has risk ownership, significantly larger contributions are made to a wider range of strategic and operational risks.

Finally, Viscelli, Hermanson, and Beasley (2016) conducted a series of semi-structured interviews with 15 ERM champions representing 14 organizations headquartered in the United States to gain insight into how firms actually implement ERM. They found that most firms began their process by developing a list of risks. Very few of the firms provided formal education on ERM to the employees involved in the ERM implementation. Most of the organizations did not define risk appetite. The most positive ERM impact on the firm was greater risk awareness, risk management, and risk mitigation, and more timely dissemination of risk information was identified as the Number 1 change to the firm.

Key implications for boards. A key "takeaway" from our analysis of ERM research to address our second question of interest (*What techniques comprise an ERM process?*) is that there is no one specific approach used by organizations to implement ERM. While several organizations mentioned they have found some benefit in considering aspects of an ERM framework, such as COSO (2004), our review of the

research suggests that organizations approach the launch of ERM in a number of different ways, and they have not focused on implementing all elements laid out in an ERM framework. Some start by leveraging existing processes, while others start by appointing individuals to serve in new CRO roles or they create a RMC among the executive team to launch the process. But, one common aspect noted in several studies is that most organizations engaged management in an initial risk identification task early in an ERM launch, and a number of those organizations used "heat maps (risk maps)" to summarize the most important risks identified.

Opportunities for future research. The limited access to data about specific techniques and internal processes used by organizations as they implement ERM has limited the ability to conduct academic research about the effectiveness of those processes. There is limited knowledge about specific factors that may affect the effectiveness of any number of ERM processes. Research that sheds insights into tools and techniques, including both their advantages and disadvantages, would be extremely beneficial to better understand factors that strengthen an entity's overall risk oversight. As researchers can gain access to data about specific ERM implementations, there are a number of important research questions specific to ERM implementation processes that warrant academic study by governance scholars. We summarize a number of research questions related to ERM implementations in column B of Appendix A.

Internal Auditing and ERM

In response to growing expectations for more effective board risk governance, a number of boards have called upon IA to assist them with their ERM efforts. In many organizations, the audit committee of the board is responsible for oversight of the IA function, and there are direct lines of communication between IA and the board via the audit committee. Because IA has an enterprise-wide focus and because IA procedures are often risk-based, a number of boards of directors have initially assigned responsibility for ERM leadership to IA. However, in doing so, some boards may question what IA's role in ERM should be, and they may have concerns about how ERM leadership affects IA's objectivity.

The IA function, especially the chief audit executive, is frequently tasked with the leadership of ERM implementation (Viscelli et al., 2016). While there is disagreement in the IA community about how closely the Institute of Internal Auditors (IIA; 2004) guidelines about IA involvement in ERM should be followed, there is agreement that IA should never "own" risk, because owning the risk would jeopardize IA's independence and objectivity in evaluating risk (Jackson, 2005). Several articles discuss the appropriate role of the IA function in ERM.

The IIA released a position paper, *The Role of Internal Auditing in Enterprise-Wide Risk Management* (IIA, 2004), shortly after COSO (2004) released its ERM framework. The IIA provided guidance on the roles internal auditors should or should not perform in risk management, and it stated that IA's core role is to "provide objective assurance to the board on the effectiveness of risk management" (p. 3). Some practice-based polls of IA practitioners provide some insights about consistency with the IIA guidelines. For example, Gramling and Myers (2006) found in a survey that the responsibilities held by internal auditors differed somewhat from The IIA's guidelines, but that internal auditors understood the guidance. Also, Sobel (2011) surveyed IIA members through the IIA's Global Audit Information (GAIN) Flash system and found that IA was not participating in core ERM roles, consistent with IIA guidelines on ERM implementation. In addition, Thompson (2013) provided a framework that can be used to evaluate the potential conflicts that an internal auditor might face while implementing ERM.

Fraser and Henry (2007) found in a study of U.K. companies that internal auditors were playing a bigger role in ERM than recommended by the IIA, and there was concern that they were doing so at the risk of losing independence. Interviews revealed that internal auditors were in the role of risk management facilitators and consultants, rather than evaluators of risk management processes. This raised the question of whether the internal auditors were maintaining their independence.

Beasley, Clune, and Hermanson (2008) focused on the macro-level impact of ERM on IA. They surveyed 122 firms and found that, overall, ERM implementation positively affects IA by expanding IA's work as the organization progressed through its implementation. This is not surprising, as ERM implementation requires significant resources, and, as outlined by The IIA's guidelines, there are many roles for IA in the process. The authors also found a greater impact on IA by ERM when the CFO and audit committee have called for IA to have greater involvement in the ERM process and when IA has a greater role in leadership of the ERM implementation. This suggests that CFOs and audit committees may recommend that IA take a leadership role, thus leading to an impact on IA resources, which could lead to a loss of independence. The authors did not conclude whether greater IA involvement in ERM was helpful or harmful to IA's independence and objectivity.

Key implications for boards. Our analysis of ERM research to address our third question of interest (*What is the role of IA in ERM?*) indicates that IA has played an active role in the initial launch of ERM in a number of organizations. In some ways, this is not surprising given the board of directors often delegates day-to-day responsibility for the board's risk oversight to the audit committee. Because the audit committee has direct oversight responsibility over IA, it is not surprising that boards, through their audit committees, have asked IA to assume some ERM leadership. However, that has led to concerns about continuing to use IA in an ERM leadership role. A number of studies have called attention to the impact of IA's leadership of ERM on its ability to

objectively evaluate the functioning and effectiveness of the organization's ERM processes. Boards may benefit from considering whether IA should continue in its ERM leadership role.

Opportunities for future research. Because many ERM implementations have been facilitated by internal auditors, there are a number of research questions related to the impact of that reality. Although most IA functions use a risk-based approach to their audit scoping, it is uncertain the extent to which IA activities focus on risks beyond operations, financial reporting, and compliance into those risks related to strategy. In addition, while there are concerns about the potential compromising of IA objectivity and independence when IA assumes responsibility for ERM implementation, there is limited research as to whether that concern can be empirically supported. In response, we summarize, in column C of Appendix A, a number of future research questions that governance scholars could examine to provide additional insights about the role of IA in ERM.

Research Insights Related to Board's Evaluation of Risk Information Generated by ERM Processes

In addition to responsibilities related to understanding and approving management's approach to risk oversight, boards also are responsible for understanding risk information output from the ERM process as part of the board's oversight of management. Conceptually, ERM is a process designed to increase the likelihood that entity objectives are achieved (COSO, 2004). Thus, ultimately, ERM is designed to provide strategic value. But, as boards evaluate information generated by ERM processes in organizations they serve, they may have questions about how organizations integrate ERM with the strategy of the organization, and they may ask whether ERM processes actually enhance stakeholder value. We examine ERM-related research to summarize insights to these governance questions:

a. How are organizations integrating ERM processes with strategy?
b. How does ERM affect firm value and performance?
c. How does organizational culture affect the value of ERM?

We use these questions as a framework for organizing our understanding of insights from ERM-related research performed to date and we build upon that to generate a number of future research topics that governance scholars may consider for future examination.

ERM and Strategy

The COSO (2004) framework emphasizes that ERM is a process "applied in strategy setting" designed "to provide reasonable assurance regarding the achievement of entity objectives" (p. 2). That definition indicates that ERM is intended to focus on the management of risks affecting the strategy a firm uses to achieve its objectives. Similarly, Frigo and Anderson (2011) stated that ERM must take place within a strategic setting to actually create value.[4] Despite these assertions, the academic literature indicates that firms typically are struggling to effectively link ERM to strategy.[5]

Beasley, Branson, and Pagach (2015) examined firm-specific factors associated with the perceived strategic value of ERM, using a sample of 645 organizations across a number of industries. They found that ERM is more likely to be viewed as a strategic tool when the organization has stated its risk appetite in the strategic planning process and when the board of directors receives, at least annually, a management report describing top risks. As for management-level processes, they found greater linkage of ERM and strategy when the organization has a management-level risk committee, provides ERM training to executives, and regularly updates the key risk inventories. Interestingly, they also found that the presence of an explicit relationship between executive compensation and risk management increases the perceived strategic value of ERM. In addition, larger firms were more likely to view ERM as a strategic tool, while private firms were more likely than public firms to view ERM as value adding.

Cohen, Krishnamoorthy, and Wright (2014) interviewed CFOs, audit committee members, and audit partners within the same firms (which they referred to as the governance triad) for 11 organizations. They found that CFOs and audit committee members more often included strategic elements in their definition of ERM than did audit partners. In only two of the organizations did all three members of the governance triad mention strategy. Of the remaining organizations, half had triads where the majority of the triad members noted strategy in their responses, and in most of those triads, the audit committee member and the CFO were the ones noting the strategy connection most often. When asked about their individual role in addressing risks related to the four objectives (strategic, operational, reporting, and compliance) outlined in the COSO (2004) ERM framework, the CFOs and the audit committee members were more likely to respond that they played a significant role in assessing risks related to the strategic objective. The external auditors saw their role as weak in the assessment of risks related to the strategic objective. The authors also reviewed the responses through the lens of agency theory and resource dependence theory. While they found that ERM was mostly playing a monitoring role (agency theory), they did see it being used to balance corporate strategy and business risks (resource dependence) in some cases.

Viscelli et al. (2016) interviewed ERM champions in 14 organizations and found that most of the organizations adopted ERM due to a "strategic need to understand risk." However, the most common area cited by interviewees for future improvement in the ERM process was

the link to strategic planning, and making ERM more a part of the organization's strategy was cited when asked about goals for the ERM implementation over the next 3 to 5 years. Overall, the responses seem to indicate that ERM's strategic impact is limited and that the ERM implementation process often begins with a resource dependence/strategic focus, but ultimately emerges as more of an agency theory/monitoring tool. As a result, the overall impact of ERM is limited by the failure to tightly link ERM and strategy.

In a study of 110 non-financial Canadian firms, Ben-Amar, Boujenoui, and Zéghal (2014) found that a firm's risk management approach is directed by the firm's corporate strategy. Content analysis was performed on annual reports for 2007 to examine risk management. The authors reported that a firm's business sector affects the risk exposure level, perception of risk consequences, and risk management strategy for both individual risks and risk categories.

Key implications for boards. A key "takeaway" from our analysis of ERM research to address our fourth question of interest (*How are organizations integrating ERM processes with strategy?*) is that while ERM is envisioned to provide an organization the opportunity to identify and manage risks most likely to affect the organization's achievement of its strategic objectives, the integration of ERM and strategy has not been fully achieved, and organizations are struggling to fully leverage the strategic benefits of ERM. Organizations that have realized some strategic benefit are found to have boards of directors more engaged in the risk governance process.

Opportunities for future research. Future research is needed on the processes and activities used to incorporate ERM into strategic planning, the related keys to how organizations have successfully connected risk management and strategic planning, and the extent that ERM is considered a priority for running the business. We summarize in column A of Appendix B a number of research questions related to the integration of ERM and strategy that can be examined by governance scholars to provide insight to boards to help them properly position risk governance for strategic value.

Firm Value and Performance

As noted in the COSO definition of ERM, the goal of an effective ERM process is to increase the likelihood that organizations achieve their objectives. Although that is conceptually appealing, a number of boards may question whether actual ERM implementations have demonstrated value-adding contributions.[6] To explore answers to that question, we examine prior ERM research for insights about the association of ERM with firm value and performance.

Nocco and Stulz (2006) argued that the implementation of an integrated, holistic risk management environment (ERM) can be used to create value by better managing risk at a macro and micro level. By looking across the enterprise's risks and coordinating them, ERM helps to ensure that no single project has a negative impact on the firm (Stulz, 1996). Unlike Nocco and Stulz (2006), Schiller and Prpich (2014) argued that ERM is lacking in solid empirical validation that the comprehensiveness is worth the effort, and its adoption is limited by its lack of solid theoretical support. The authors also point out that ERM does not provide institutional design recommendations.

While ERM has been widely accepted, there has been some resistance to the value proposition of ERM. For example, Power (2009) argued that ERM encourages a "logic of auditability," which results in process-based rules with an ever-expanding reach leading to "the risk management of everything" (Power, 2004). The author also argues that the narratives of risk management cannot articulate nor comprehend the interconnectedness of critical risks. Power (2009) suggested that business continuity management (BCM) is a better way to manage risk because it potentially has a better consideration of interconnectedness. Overall, Power (2009) suggested that ERM ultimately can lead to the "risk management of nothing." These views illustrate how some question whether ERM has the potential to be value adding.

Beasley, Pagach, and Warr (2008) used announcements of appointments of senior executives into ERM roles such as CRO to proxy for the launch of ERM. In a sample of 120 announcements of a senior executive being appointed to an ERM role, they found that there are significant relations between the magnitude of abnormal returns for the 2-day period surrounding the announcement and certain firm-specific characteristics. The authors state,

> For nonfinancial firms, announcement period returns are positively associated with firm size and the volatility of prior periods' reported earnings and negatively associated with leverage and the extent of cash on hand relative to liabilities. For financial firms, however, there are fewer statistical associations between announcement returns and firm characteristics. (pp. 311-312)

Overall, the study found that the value of ERM is dependent on the overall risk profile of the firm, with shareholders of higher risk firms placing greater value on the announcements of CRO appointments relative to other firms.

Gordon, Loeb, and Tseng (2009) used a word search to identify 122 firms that disclosed ERM activities. Using Compustat data to measure strategy, operations, reporting, and compliance (the four objectives in COSO's ERM Framework), they developed an index of the effectiveness of a firm's ERM initiative. The ERM effectiveness measure was then used in a regression with independent variables representing firm characteristics.[7] The authors used a subsample of high performance firms, as measured by 1-year excess stock returns (2% or better), to establish coefficients (best practices) of the firm characteristics of high performing firms. The authors then developed an optimum ERM score, which was compared with actual ERM

scores. They found that the smaller the difference in optimum score and actual score, the greater the expected performance. The results of the study indicated that firms whose ERM initiative characteristics were properly aligned with the firm's characteristics should experience greater firm performance.

Hoyt and Liebenberg (2011) performed a similar word search as Gordon et al. (2009) to identify insurance firms between 1998 and 2005 that had ERM initiatives. Using Tobin's *Q* as a proxy for firm value, they found that firms with an ERM initiative had a higher median change in value than firms without an ERM initiative. On average, their results showed that firms with ERM initiatives were valued approximately 4% higher than firms without an ERM initiative. However, unlike Hoyt and Liebenberg (2011), Lin et al. (2012) found that the market responded negatively to ERM adoption in a study of insurance firms using Tobin's *Q* and a similar word search to identify ERM adoption.

McShane, Nair, and Rustambekov (2011) also used Tobin's *Q* as a proxy for firm value and the S&P ERM rating. The authors found that insurance firms experienced an increase in firm value as the firms increased their risk management sophistication in traditional risk categories. As the firms moved beyond silo risk management to a coordinated (holistic) approach, the firms did not see an increase in firm value. This suggests that firms achieve a higher level of performance as the firm improves overall risk management and controls, but further performance improvement is not apparent as firms move into more advanced ERM processes.

Gupta, Prakash, and Rangan (2012) examined 73 publicly traded firms, using a word search (1999-2009) to find the announcement of a CRO, and found that the market was more likely to react positively, as measured by increase in stock price, if the organization had few outside directors, suggesting that CRO appointments may lead to better governance.

Nair, Rustambekov, McShane, and Fainshmidt (2014) examined 60 insurance firms during the 2008 financial crisis to determine if the ERM processes align with the dynamic capabilities of the firm, allowing firms to better manage a changing environment. They calculated the stock decline between October 9, 2007 (S&P peak) and March 6, 2009 (S&P lowest point). Profitability return was calculated from the lowest point and post-crisis high in April 2011. Using the S&P rating, translated to a scale of 1 (*weak*) to 5 (*excellent*), they found that a superior ERM rating (5) resulted in a smaller stock decline during the downturn and superior profitability during the recovery period.[8]

Baxter et al. (2013) examined 165 insurance and banking firm-years that received ERM ratings from S&P from 2006 to 2008 to investigate the rating in relation to firm performance as measured by return on assets (ROA) and Tobin's *Q*. They found that firms with a higher ERM rating had higher operating performance (ROA) and higher Tobin's *Q*s. The authors attributed this to ERM helping to mitigate risks and/or allowing the firms to take advantage of opportunities. The study also found that firms receiving a strong/excellent ERM rating initially had a stronger market reaction to the disclosure of the rating than those with lower ratings. In addition, they considered the time period before the global financial crisis, during the crisis, and after the crisis. They found a strong relationship between higher ERM ratings and market value only after the crisis and attributed this to investors looking for information such as the ERM rating to provide insight into a firm's ability to address future risks.

In an additional study evaluating ERM maturity and firm value as measured by Tobin's *Q*, Farrell and Gallagher (2015) used the Risk Management Society (RIMS) risk maturity model (RMM) to evaluate whether ERM maturity had an impact on firm value. Using the results collected from 2006 to 2011, which resulted in 225 firms across various industries, the authors found that there is significant evidence that ERM maturity has a positive impact on firm value. For firms with an overall RMM score of 3 to 5 (mature), firm value increased 25% and was highly significant as measured by Tobin's *Q*. All of the areas of the RMM online tool were found to affect value, except risk appetite management and business resilience and sustainability.

In a study of U.S. insurers who answered the Tillinghast Powers Perrin ERM survey of 2004 and 2006, Grace, Leverty, Phillips, and Shimpi (2015) studied cash flow implications of the adoption of ERM and found that organizations having a cross-functional dedicated risk manager who reported to the board or CEO, along with a simple economic model, had significant increases in revenue and cost efficiency.

Key implications for boards. Our analysis of ERM research to address our fifth question of interest (*How does ERM affect firm value and performance?*) reveals evidence that implementations of ERM do affect positively different measures of firm value. Some studies find stock market reactions to ERM implementation announcements, while others (but not all) find a relationship between ERM and firm value as measured by Tobin's *Q*. Thus, there is empirical evidence that there is a connection between ERM and value creation.

Opportunities for future research. Because questions about the value relevance of ERM are often posed by boards of directors and senior executives who may be reluctant to embrace ERM as an effective risk oversight technique, further research is needed that might help to demonstrate whether, or when, ERM provides value to organizations. While there is some research that suggests ERM does provide measurable value, more research is needed to expand our understanding of the various dimensions of value for ERM. We summarize in column B of Appendix B a number of research questions that governance scholars could examine in future research.

Culture and ERM

Three of the major organizational change initiatives of recent decades, reengineering, total quality management (TQM),

and firm downsizing, have had less than stellar success (Cameron & Quinn, 2006). Lack of organizational culture fit to an initiative was given as a common reason for failure, leading to the belief that an organization's culture and strategy must be aligned to be successful. As ERM is a change initiative similar to the previously mentioned initiatives, it is reasonable to assume that an organization's culture would be a significant factor in explaining the strategic value of ERM.

Mikes (2009) found in a longitudinal study of two banks that two cultures emerged, "ERM by the Numbers," driven by a strong shareholder value imperative, and "Holistic ERM," driven by a risk-based internal-control imperative. The ERM by the Numbers firm relied heavily on calculations for quantitative risks, which resulted in a *diagnostic* risk model. The Holistic ERM firm quantified risks but did not rely solely on the numbers. Also, senior risk managers with intimate knowledge of the business sectors responded to management's concerns and thus influenced the actions beyond what the numbers might have shown.

In a follow-on study, Mikes (2011) interviewed 53 individuals in risk management positions at five major banks over the period of 2001-2010. The article sought to determine if the pursuit of expanding risk measurement in risk management was leading to a dysfunctional environment, as espoused by Power (2009) and Tabel (2007), and if the type of culture as defined in Mikes (2009) explained why some organizations become committed to risk measurements, whereas others do not. The author used boundary-work to suggest that organizations that are "ERM by the Numbers" create risk measurements that imply the expertise on risk lies in the risk organizations and can lead to greater organizational control. Mikes described these organizations as having "quantitative enthusiasm" and being dedicated to risk measurements. Organizations that approach ERM in a holistic manner focus on combining risk measures with experience and intuition to develop soft measurements, which better reflect the risk of non-measurable strategic risks. The approach seems to leave the boundaries blurred as to where the expertise lies in an organization. These organizations were described as having "quantitative skepticism" and providing top management with alternative scenarios on emerging risks.

Cooper, Faseruk, and Khan (2013) performed a meta-analysis of practitioner studies to determine the relationship between ERM and organizational culture. By grouping relevant questions from 14 major risk studies published from 2006 through 2010, the authors analyzed the responses from the perspective that organizational culture was a "major benefit" or a "major barrier" to implementation of ERM. Their study did not put forth an answer to this question but did find that a significant number of entities consider organizational culture important to ERM implementation.

A common way of describing organizational culture is on a continuum from mechanistic to organic (Burns & Stalker, 1961). Mechanistic cultures have a chain of command structure in the form of rankings of positions, vertical communication paths, and decisions driven down to employees from top management. On the other end of the continuum, organic cultures have a network of control and authority, lateral communication paths, and employees who receive information and advice in a cooperative manner rather than instructions from supervisors.

Kimbrough and Componation (2009) used an instrument, Organizational Culture Assessment (OCA; Reigle, 2001, 2003), which was based on the mechanistic/organic continuum of Burns and Stalker (1961), to study how the organizational culture framework is related to ERM implementation. In a study of 116 firms from 21 different industries, the authors found that organizations with higher organic scores were more likely to have a risk management program, were more likely to state that culture aided in the speed and effectiveness of ERM implementation, and were more satisfied overall with the effectiveness of the firm's ERM program. Firms with higher OCA scores (organic culture) were more likely to answer "yes" to the question of whether the firm's culture has been modified to support ERM. This finding is not surprising given that organic firms are more open to change and innovation. The study did not find that culture was related to the presence of a CRO, but for the firms that did have a CRO, the firms with organic cultures were more likely to have a formal risk management process and to be further along in the ERM implementation. Similarly, Kleffner, Lee, and McGannon (2003) found that a hindrance to ERM adoption was a silo mentality at firms due to the firms' organizational structure, which could be interpreted as a characteristic of a mechanistic culture.

Key implications for boards. A key "takeaway" from our analysis of ERM research to address our final question of interest (*How does organizational culture affect the value of ERM?*) is that organizational culture has a significant impact on the decision to implement ERM and on the effectiveness of that implementation. Some have argued that "culture is king" when it comes to ERM. Without sufficient support of ERM by the CEO or board of directors, organizations may struggle in their efforts to find strategic value in their ERM processes. Thus, boards may need to consider the organization's culture as it evaluates the effectiveness of management's risk management processes.

Opportunities for future research. Because research about the role of culture in the context of ERM is limited, additional studies are warranted to answer the question as to how organizational culture influences an ERM implementation. Research about elements of culture that affect the overall effectiveness of ERM is needed to help boards and senior executives in their efforts to implement risk oversight processes that help them navigate risks that may be on the horizon. We summarize in column C of Appendix B a number of potential research questions related to the role of culture in ERM that governance scholars may want to examine.

Conclusion

ERM is emerging corporate governance topic, particularly for boards of directors as they respond to increasing expectations

for more effective risk governance. ERM has become a major focus of many organizations because of legislation and regulations, as well as recent corporate failures. While the academic research related to ERM is emerging, it is still in its early stages. Despite that, we believe that there are a number of key insights from research conducted to date that boards may benefit from considering. We have highlighted a number of those in this article and in Table 1. We also believe that there are many other potential research questions that warrant rigorous academic study by governance scholars. In this article, we have identified a number of research questions in Appendices A and B related to the two primary ERM-related responsibilities of the board of directors.

In some ways, the academic world's embrace of ERM has lagged the business world. There is tremendous opportunity for researchers to contribute insights that would be highly relevant to business leaders, and this study attempts to provide motivation to encourage scholars to continue their examination of a number of issues that can inform key governance players, including the board of directors and audit committee, in their risk governance efforts.

Research is needed along multiple dimensions of ERM, and expertise bridging a number of academic fields is needed. Because ERM is intended to oversee risks arising across the enterprise, academic experts in a variety of business disciplines (i.e., accounting, finance, information technology [IT], marketing, strategy, and organizational behavior), in addition to experts in disciplines beyond business (i.e., economics, sociology, psychology, industrial engineering, computer science, statistics, and data analytics) have significant opportunities to contribute to our understanding of ERM. More importantly, research that integrates academic analysis of business and non-business disciplines can provide unique insights about what works well and what does not in managing the volume of complex risks facing enterprises. Because organizations will always face risks in the pursuit of value, organizations will constantly be seeking insights about more effective techniques to proactively manage the risks that may emerge. The academic community is uniquely positioned to assist with providing rigorous analyses that will provide insight into the effectiveness of ERM processes. The landscape of research questions related to ERM is open and diverse. The academic community needs to take advantage of this significant opportunity.

Appendix A

Summary of Research Opportunities to Address Board's Understanding and Approval of ERM Processes.

Column A	Column B	Column C
Research opportunities to address, "What types of organizations implement ERM?"	Research opportunities to address, "What techniques comprise an ERM process?"	Research opportunities to address, "What is the role of IA in ERM?"
1. To what extent do prior risk events affecting the firm affect the decision to adopt ERM? 2. How are regulators affecting an entity's decision to implement ERM, and how might regulations explain ERM adoptions in different industries? 3. What role does the board of directors play in encouraging ERM adoption? 4. How do differences in ownership structures, including shares held by directors, senior management, and institutional investors, affect ERM adoption? 5. How does the embrace of ERM by competitors explain a firm's adoption of ERM? 6. To what extent does the life cycle of an industry or firm explain the need for ERM? 7. How does the level of diversification of an entity affect its decision to embrace ERM? 8. What additional measures are available to proxy for ERM implementation? 9. How does executive compensation affect a firm's decision to embrace ERM? 10. To what extent are ERM implementations affected by the types of executives responsible for leading risk oversight in the organization?	1. What attributes affect the embrace of a particular ERM conceptual framework, and why are frameworks important to ERM champions in an organization? 2. How might existing theories in the academic literature be used to strengthen ERM frameworks, and how might ERM frameworks be used to inform the development of new theoretical arguments for ERM? 3. How do organizations organize ERM processes across complex, global enterprises? 4. How are organizations aggregating risks to create an enterprise-wide portfolio of risks? 5. What techniques are organizations using to help leaders of specific business functions recognize how their efforts to reduce risks in their function actually may create risks for other functions in the enterprise? 6. What techniques are entities using to engage executives in processes to prioritize risks? 7. What processes are organizations using to assess the existence and adequacy of responses to top risks to the organization? 8. How are organizations assigning ownership to executives for each of the top risk exposures identified by the ERM process? 9. How might executive compensation create incentives for excessive risk taking that is beyond the entity's appetite for risk? 10. How are organizations considering interrelationships (i.e., correlations) among individual top-tier risks identified by the ERM process? 11. How are organizations developing KRIs to monitor changing risk conditions? 12. How are organizations communicating top risks to the board of directors?	1. What are the typical ERM processes performed by IA, and what tasks are they not performing? 2. How do varying levels of involvement by IA in ERM processes affect perceptions of IA's objectivity and independence? 3. What techniques are boards of directors and audit committees using to monitor whether IA is compromising its objectivity by performing ERM functions? 4. How do perceptions of ERM's value differ when ERM is led by IA vs. by other executives in the firm? 5. To what extent are IA functions being asked to perform objective assessments of the organization's ERM processes? 6. How is the output of ERM affecting the nature and extent of IA's audit work for the enterprise? 7. Because ERM is focused heavily on emerging risks related to strategy, to what extent is IA able to respond to strategic risks? 8. To what extent are IA functions adjusting their staffing to include individuals with experience beyond traditional IA roles that focus on financial reporting or operational and compliance issues? 9. How are the results of IA involvement in ERM processes affecting external auditor assessments of and reliance on IA in financial statement and internal control audits?

Note. ERM = enterprise risk management; KRI = key risk indicator; IA = internal audit.

Appendix B

Summary of Research Opportunities Related to Board Evaluation of ERM Output for Strategic Advantage.

Column A	Column B	Column C
Research opportunities to address, "How are organizations integrating ERM processes with strategy?"	Research opportunities to address, "How does ERM affect firm value and performance?"	Research opportunities to address, "How does organizational culture affect ERM?"
1. How are organizations embedding explicit, structured risk management processes into the strategic planning processes? 2. To what extent are organizations factoring in risk dimensions when allocating capital to specific strategic initiatives? 3. To what extent are entities using quantitative techniques, such as VAR, earnings at risk, and cash flow at risk, to assess ranges of potential risk outcomes? 4. How are organizations taking output from an entity's ERM process as input to the next round of strategic planning? 5. If the organization is mostly focused on short-term risks and strategies, how is the organization monitoring risks that may be emerging in the long term that might undermine the organization's core business model? 6. What techniques are organizations using to assess and incorporate macroeconomic and geopolitical risk conditions into their strategic planning process? 7. To what extent are organizations aligning executive leadership of their ERM processes with executive leadership of their strategic planning processes? 8. How are organizations developing and communicating the organization's appetite for risk taking? 9. How are organizations creating risk limits to ensure that management is not exposing the entity to risks beyond acceptable levels in the pursuit of strategic objectives? 10. What techniques are boards of directors using to monitor whether management is taking excessive risks in the pursuit of strategic objectives?	1. What firm characteristics and conditions are associated with increases in firm value when entities engage in ERM? 2. What types of ERM implementation techniques lead to greater value enhancements? 3. To what extent does the value of ERM differ across different industries and firm life cycles? 4. To what extent do findings about the value of ERM differ across different measures of value (i.e., cumulative abnormal returns, Tobin's *Q*, etc.)? 5. How is the value of ERM perceived differently by different stakeholders (e.g., bondholders, stockholders, regulators)? 6. What types of non-quantitative measures (i.e., qualitative perceptions of senior management, boards of directors, regulators) capture the value of ERM, and do those measures suggest value even if more traditional quantitative measures (i.e., cumulative abnormal returns, Tobin's *Q*, etc.) do not? 7. What techniques are being used by organizations to demonstrate the value of ERM? 8. How might assessments of ERM at counterparties (e.g., suppliers, customers, joint venture partners) provide value in key business decision making? 9. To what extent do the characteristics, position, and experience of the individual who serves as the internal risk champion (i.e., a Chief Risk Officer) affect perceptions of value of ERM for the organization? 10. How does the level of ERM embrace and engagement by the board of directors and the CEO affect the overall value proposition of ERM? 11. How does the effect of a prior material risk event affect the perceived value of ERM?	1. How is risk culture defined, and what are the key elements of risk culture that lead to more effective ERM? 2. What types of organizational cultures are associated with more effective and value-adding ERM processes? 3. How does the manner in which the board of directors structures its risk oversight responsibilities affect the attitude and tone at the top regarding ERM? 4. How do the title and position of the ERM leader affect the culture and embrace of ERM? 5. What actions by the CEO help to support a strong risk oversight culture vs. a weak culture? 6. How does the overall risk culture affect the value perceptions of ERM or the integration of ERM with strategy? 7. How does risk culture change over time as the organization experiences different events? 8. What are the typical cultural barriers that limit the embrace and development of ERM within an organization?

Note. ERM = enterprise risk management; VAR = value at risk.

Authors' Note

This article is partly derived from the first author's dissertation at Kennesaw State University.

Acknowledgments

The authors thank Daniel Street for research assistance.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research and/or authorship of this article.

Notes

1. For example, Acharyya and Johnson (2006) interviewed four insurance companies and found the answers so diverse that they concluded the implementation of enterprise risk management (ERM) varies widely.
2. The components were (a) processes for identifying, assessing, and prioritizing risks; (b) frequency of risk meetings; and (c) risk tools. The types of risk were (a) preventable, (b) strategy execution, and (c) external (as proposed by Kaplan & Mikes, 2012).
3. The survey questions measured eight components: (a) objective setting, (b) risk identification, (c) risk reaction, (d) oversight, (e) information and communication, (f) internal environment, (g) management, and (h) performance.
4. Funston (2004) found that of the 100 companies with the biggest stock-price loss during 1995 to 2004, 66 experienced strategic risks and 80% of the largest loss firms experienced two or more interrelated risks. Slywotzky and Drzik (2005) argued that companies are becoming better at managing overall corporate risks but have yet to address the management of strategic risks.
5. Gates (2006), in a survey of 271 The Conference Board members, found that 66% of the firms were implementing ERM to foster a greater understanding of strategic risks but were more willing to accept strategic risks over more traditional risks, such as legal or financial risks.
6. Kraus and Lehner (2012) reviewed the ERM literature on value creation. They found that there is a lack of reliable proxies for

value and an inability to determine what part of ERM influences value.

7. The independent variables used were environmental uncertainty (earnings volatility), industry competition (highly competitive), firm size (total assets), firm complexity (diversity of business transactions), and monitoring by the board (size of board divided by the log of sales).
8. Aebi, Sabato, and Schmid (2012) found that banks with a chief risk officer (CRO) who reported to board instead of the CEO exhibited higher stock returns and return on equity (ROE) during the 2007/2008 financial crisis than firms whose CRO reported the CEO. Eckles, Hoyt, and Miller (2014) found that insurance companies that adopted ERM experienced a reduction in stock volatility that gradually grew over time.

References

Aabo, T., Fraser, R., & Simkins, B. (2005). The rise of the chief risk officer: Enterprise risk management at Hydro One. *Journal of Applied Corporate Finance*, *17*(3), 62-75.

Acharyya, M., & Johnson, J. (2006, July). Investigating the development of enterprise risk management in the insurance industry: An empirical study of four major European insurers. *The Geneva Papers on Risk and Insurance: Issues and Practice, Special Issue*, 55-80.

Aebi, V., Sabato, G., & Schmid, M. (2012). Risk management, corporate governance, and bank performance in the financial crisis. *Journal of Banking & Finance*, *36*, 3213-3226.

Arena, M., Arnaboldi, M., & Azzone, G. (2010). The organizational dynamics of enterprise risk management. *Accounting, Organizations and Society*, *35*, 659-675.

Arena, M., Arnaboldi, M., & Azzone, G. (2011). Is enterprise risk management real? *Journal of Risk Research*, *14*, 779-797.

Arnold, V., Benford, T. S., Canada, J., Kuhn, J. R., Jr., & Sutton, S. G. (2007). The unintended consequences of Sarbanes-Oxley on technology innovation and supply chain integration. *Journal of Emerging Technologies in Accounting*, *4*, 103-121.

Baxter, R., Bedard, J. C., Hoitash, R., & Yezegel, A. (2013). Enterprise risk management program quality: Determinants, value relevance, and the financial crisis. *Contemporary Accounting Research*, *30*, 1264-1295.

Beasley, M., Branson, B. C., & Hancock, B. V. (2015). *Report of the current state of enterprise risk oversight: Update on trends and opportunities* (6th ed.). Raleigh: American Institute of Certified Public Accountants/North Carolina State University. Available from www.erm.ncsu.edu

Beasley, M., Branson, B. C., & Pagach, D. (2015). An analysis of the maturity and strategic impact of investments in ERM. *Journal of Accounting and Public Policy*, *34*, 219-243.

Beasley, M., Clune, R., & Hermanson, D. R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy*, *24*, 521-531.

Beasley, M., Clune, R., & Hermanson, D. R. (2008). The impact of enterprise risk management on the internal audit function. *Journal of Forensic Accounting*, *9*, 1-20.

Beasley, M., Pagach, D., & Warr, R. (2008). Information conveyed in hiring announcements of senior executives overseeing enterprise-wide risk management processes. *Journal of Accounting, Auditing & Finance*, *23*, 311-332.

Ben-Amar, W., Boujenoui, A., & Zéghal, D. (2014). The relationship between corporate strategy and enterprise risk management: Evidence from Canada. *Journal of Management and Strategy*, *5*(1), 1-17.

Bromiley, P., McShane, M., Nair, A., & Rustambekov, E. (2015). Enterprise risk management: Review, critique, and research directions. *Long Range Planning*, *48*, 265-276.

Burns, T., & Stalker, G. M. (1961). *The management of innovation*. London, England: Tavistock Publications.

Cameron, K. S., & Quinn, R. E. (2006). *Diagnosing and changing organizational culture*. San Francisco, CA: Jossey-Bass.

Cohen, J., Krishnamoorthy, G., & Wright, A. (2014). *Enterprise risk management and the financial reporting process: The experiences of audit committee members, CFOs, and external auditors* (Working paper). Boston, MA: Boston College.

Colquitt, L. L., Hoyt, R. E., & Lee, R. B. (1999). Integrated risk management and the role of the risk manager. *Risk Management and Insurance Review*, *2*(3), 43-61.

Committee of Sponsoring Organizations of the Treadway Commission. (2004). *Enterprise risk management—Integrated framework*. New York, NY: Author.

Cooper, T., Faseruk, A., & Khan, S. (2013). Examining practitioner studies to explore ERM and organizational culture. *Journal of Management Policy and Practice*, *14*(1), 53-68.

Dodd-Frank Act of 2010. (2010). *Public Law 111-203*. Washington, DC: Government Printing Office.

Eckles, D. L., Hoyt, E. H., & Miller, S. M. (2014). The impact of enterprise risk management on the marginal cost of reducing risk: Evidence from the insurance industry. *Journal of Banking & Finance*, *43*, 247-261.

Farrell, J. (2003). A broad view of section 404. *Internal Auditor*, *60*(4), 88-89.

Farrell, M., & Gallagher, R. (2015). The valuation implications of enterprise risk management maturity. *The Journal of Risk and Insurance*, *82*, 625-657.

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

Frigo, M. L., & Anderson, R. J. (2011). Strategic risk management: A foundation for improving enterprise risk management and governance. *The Journal of Corporate Accounting & Finance*, *22*(3), 81-88.

Funston, R. (2004, April 11). Avoiding the value killers. *Treasury and Risk Management*, 11.

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

Gates, S., Nicolas, J., & Walker, P. (2012). Enterprise risk management: A process for enhanced management and improvement. *Management Accounting Quarterly*, *13*(3), 28-38.

Gordon, L. A., Loeb, M. P., & Tseng, C.-Y. (2009). Enterprise risk management and firm performance: A contingency perspective. *Journal of Accounting and Public Policy*, *28*, 301-327.

Grace, F. G., Leverty, J. T., Phillips, R. D., & Shimpi, P. (2015). The value of investing in enterprise risk management. *The Journal of Risk and Insurance*, *82*, 289-316.

Gramling, A. A., & Myers, P. M. (2006). Internal auditing's role in ERM. *Internal Auditor*, *63*(2), 52-58.

Gupta, M., Prakash, P., & Rangan, N. (2012). Governance and shareholder response to chief risk officer appointments. *The Geneva Papers*, *37*, 108-124.

Hayne, C., & Free, C. (2014). Hybridized profession groups and institutional work: COSO and the rise of enterprise risk management. *Accounting, Organizations and Society*, *39*, 309-330.

Hines, C. S., & Peters, G. F. (2015). Voluntary risk management committee formation: Determinants and short-term outcomes. *Journal of Accounting and Public Policy*, *34*, 267-290.

Hoyt, R. E., & Liebenberg, A. P. (2011). The value of enterprise risk management. *The Journal of Risk and Insurance*, *78*, 795-822.

Institute of Internal Auditors. (2004). *The role of internal auditing in enterprise-wide risk management*. Altamonte Springs, FL: Author.

Institute of Risk Management. (2002). *A risk management standard*. London, England: Author.

International Organization for Standardization. (2009). *Risk management—Principles and guidelines*. Geneva, Switzerland: Author.

Ittner, C. D., & Oyon, D. F. (2014). *The internal organization of enterprise risk management* (Working paper). Retrieved from http://ssrn.com/abstract=2486588

Jackson, R. A. (2005). Role play. *Internal Auditor*, *62*(2), 44-50.

Jordan, A., Jørgensen, L., & Mitterhofer, H. (2013). Performing risk and the project: Risk maps as mediating instruments. *Management Accounting Research*, *24*, 156-174.

Kaplan, R. S., & Mikes, A. (2012). Managing risks: A new framework. *Harvard Business Review*, *90*(6), 48-60.

Kimbrough, R. L., & Componation, P. J. (2009). The relationship between organizational culture and enterprise risk management. *Engineering Management Journal*, *21*(2), 18-26.

Kleffner, A. E., Lee, R. B., & McGannon, B. (2003). The effect of corporate governance on the use of enterprise risk management: Evidence from Canada. *Risk Management and Insurance Review*, *6*, 53-73.

Kraus, V., & Lehner, O. (2012). The nexus of enterprise risk management and value creation: A systematic literature review. *ACRN Journal of Finance and Risk Perspectives*, *12*, 91-163.

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

Lin, Y., Wen, M., & Yu, J. (2012). Enterprise risk management: Strategic antecendents, risk integration, and performance. *North American Actuarial Journal*, *16*, 1-28.

Lundqvist, S. A. (2014a). *Abandoning silos for integration: Implementing enterprise risk management and risk governance: Risk management quality and credit risk* (Dissertation, Lund University, Lund, Sweden). Retrieved from http://repository.up.ac.za/handle/2263/40635

Lundqvist, S. A. (2014b). An exploratory study of enterprise risk management: Pillars of ERM. *Journal of Accounting, Auditing & Finance*, *29*, 393-429.

Lundqvist, S. A. (2015). Why firms implement risk governance: Stepping beyond traditional risk management to enterprise risk management. *Journal of Accounting and Public Policy*, *34*, 441-466.

McShane, M. K., Nair, A., & Rustambekov, E. (2011). Does enterprise risk management increase firm value? *Journal of Accounting, Auditing & Finance*, *26*, 641-658.

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

Mikes, A. (2011). From counting risk to making risk count: Boundary-work in risk management. *Accounting, Organizations and Society*, *36*, 226-245.

Mikes, A., & Kaplan, R. S. (2014). *Towards a contingency theory of enterprise risk management* (Working paper, Harvard Business School). Retrieved from http://www.hec.unil.ch/documents/seminars/dcc/1102.pdf

Nair, A., Rustambekov, E., McShane, M., & Fainshmidt, S. (2014). Enterprise risk management as a dynamic capability: A test of its effectiveness during a crisis. *Managerial and Decision Economics*, *35*, 555-566.

National Association of Insurance Commissioners. (2013). *The U.S. national state-based system of insurance financial regulation and the solvency modernization initiative*. Washington, DC: Author.

New York Stock Exchange. (2004). *NYSE corporate governance rules § 303a*. New York: Author.

Nocco, B. W., & Stulz, R. M. (2006). Enterprise risk management: Theory and practice. *Journal of Applied Corporate Finance*, *18*(4), 8-20.

Paape, L., & Spekle, R. F. (2012). The adoption and design of enterprise risk management practices: An empirical study. *European Accounting Review*, *21*, 533-564.

Pagach, D., & Warr, R. (2011). The characteristics of firms that hire chief risk officers. *The Journal of Risk and Insurance*, *78*, 185-211.

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

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

Reigle, R. F. (2001). Measuring organic and mechanistic cultures. *Engineering Management Journal*, *13*(4), 3-8.

Reigle, R. F. (2003). *Organizational culture assessment: Development of a descriptive test instrument* (Doctoral dissertation, The University of Alabama in Huntsville). Retrieved from ProQuest Dissertations and Theses database (UMI 3079377).

Roth, J. (2006). An enterprise risk catalyst. *Internal Auditor*, *63*(1), 81-87.

Schiller, F., & Prpich, G. (2014). Learning to organise risk managements in organizations: What future for enterprise risk management? *Journal of Risk Research*, *17*, 999-1017.

Securities and Exchange Commission. (2009). *Proxy disclosure enhancements*. Washington, DC: Author.

Slywotzky, A., & Drzik, J. (2005). Countering the biggest risk of all. *Harvard Business Review*, *83*(4), 78-88.

Sobel, P. J. (2011). *Internal auditing's role in risk management*. Altamonte Springs, FL: The Institute of Internal Auditors Research Foundation.

Standard & Poor's. (2012). *Methodology: Management and governance credit factors for corporate entities and insurers*. New York, NY: Standard & Poor's Rating Services.

Stulz, R. M. (1996). Rethinking risk management. *Journal of Applied Corporate Finance*, *9*(3), 8-25.

Subramaniam, N., McManus, L., & Zhang, J. (2009). Corporate governance, firm characteristics and risk management committee formation in Australian companies. *Managerial Auditing Journal*, *24*, 316-339.

Tabel, N. (2007). *The black swan: The impact of the highly improbable*. New York, NY: Random House.

Tekathen, M., & Dechow, N. (2013). Enterprise risk management and continuous re-alignment in the pursuit of accountability: A German case. *Management Accounting Research*, *24*, 100-121.

Thompson, R. (2013). A conceptual framework of potential conflicts with the role of the internal auditor in enterprise risk management. *Accounting and Finance Research*, *2*(3), 65-77.

Viscelli, T., Hermanson, D. R., & Beasley, M. (2016). *The strategic effectiveness of ERM: Implications for corporate governance* (Working paper). Auburn, AL: Auburn University.

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

Author Biographies

Therese R. Viscelli is a visiting Assistant Professor at Auburn University. Her research focuses on Enterprise Risk Management (ERM), accounting information systems (AIS), and AIS pedagogy.

Mark S. Beasley is the Deloitte Professor of Enterprise Risk Management and the Director of the Enterprise Risk Management (ERM) Initiative at North Carolina State University. The ERM Initiative provides thought leadership about ERM practices and their integration with strategy and corporate governance.

Dana R. Hermanson is the Dinos Eminent Scholar Chair of Private Enterprise, Professor of Accounting, and Director of Research of the Corporate Governance Center at Kennesaw State University. His research focuses primarily on fraud, auditing, and governance.