Enterprise Risk Management: History and a Design-Science Proposal

Abstract

Purpose – This paper investigates the evolution of enterprise risk management (ERM) out of fragmented disciplinary perspectives to provide a foundation for promoting interdisciplinary research and proposes a design science approach for more effective ERM implementation in organizations.

Design/methodology/approach – This conceptual paper synthesizes ERM research and practice from multiple disciplines.

Findings – Corporate risk management concepts were born in academic finance and developed further in the finance subset known as risk management and insurance. With the advent of ERM, efforts must broaden beyond applying statistical models to quantifiable risks. Other disciplines have expanded ERM research by embracing techniques to investigate risk management practices to produce knowledge that integrates practice and theory. ERM is promoted as integrated risk management, yet silos still remain in both practice and research.

Originality/value – Provides a foundation and a proposal for moving ERM past academic and organizational silos, which is necessary to achieve the ERM philosophy and increase organizational resilience. Understanding the evolution and fragmented nature of ERM research and practice provides a foundation for interdisciplinary cooperation necessary to achieve the holistic ERM philosophy. A next frontier is effective ERM implementation. This paper argues for an organizational design science approach for mitigating the resistance to change that confounds effective implementation of ERM in organizations facing an increasingly uncertain environment and outlines future research for applying the approach to implementing the ISO 31000 risk management process.

Keywords Enterprise risk management, ERM, Design science, Design thinking, Change management, Organizational resilience.

Paper type Research paper

1. Introduction

Enterprise risk management (ERM) plays a corporate governance role in the holistic management of all risks to aid in decision making and increasing the likelihood of achieving operational and strategic objectives. Risks are typically classified with hazard, financial, operational, and strategic risks being four common categories (D'Arcy and Brogan, 2001; Elliott, 2013). Even though ERM scholarship has roots in the academic Finance/Risk Management and Insurance (RMI) discipline, research there has almost solely focused on hazard and financial risks. These more quantifiable types of risk suit the skills of RMI researchers, but for ERM to be truly holistic and play a strategic role in organizations, a broader research agenda must include difficult to quantify risks, such as the more ambiguous operational and strategic risks, and foundational ERM concepts, such as risk appetite, corporate governance, strategic view of risk, breaking down risk management silos, and implementation of ERM (Bharathy and McShane, 2014).

Accounting research has brought a focus on the "management" part of ERM with broad efforts on the relationship of management control and corporate governance to risk management. This research has been active in advancing risk management research beyond Finance/RMI roots by employing multiple research paradigms, such as field and case study methods, contingency theories, and actor network theory (Mikes, 2009 and 2011; Hopper and Bui, 2016). Other disciplines have contributed also. Nair *et al.* (2014) and Bogodistov and Wohlgemuth (2017) discuss ERM from a dynamic capability perspective. Gatzert and Schmit (2016) integrate the management of reputation risks into the ERM framework.

The holistic ERM philosophy requires interdisciplinary efforts that result in integration and the building of a more comprehensive perspective. A major issue facing corporate risk management is the effective implementation of ERM, which is not amenable to one-size-fits all solutions, but is contingent on factors that vary across organizations (Mikes and Kaplan, 2015). This paper proposes organizational design science to overcome the difficulty and uncertainty related to implementing ERM, which requires a major change management process involving the breakdown of functional silos. The organizational design science philosophy includes understanding stakeholders who will be directly affected and proceeds in increments with learning applied after each step. In a complex, rapidly changing environment, planning that locks in an inflexible long-term commitment can lead organizations attempting ERM implementation too far down a wrong path. In essence, organizational design science applies a continuous real options philosophy that allows regular pivots to mitigate this risk and increase organizational resilience.

To understand necessary research going forward, an understanding of how the current state was reached is essential. The next two sections summarize traditional risk management (TRM) in the academic finance/RMI literature and in practice. The subsequent section describes the currently fragmented nature of ERM practice with the goal of reducing confusion about a basic question: "What is ERM?". This paper documents the evolution of ERM out of multiple research areas, professional associations, and siloed corporate departments. Next, this paper describes

important contributions of accounting and other research to move ERM research beyond purely quantitative statistical analysis. The final section introduces the organizational design science approach and proposes its application to overcome resistance to organizational change that hinders effective ERM implementation.

2. Traditional risk management (TRM) in the academic finance literature

Risk management has a long and contentious history in academic finance research. Historically, finance scholars saw corporate risk management as value decreasing at worst and irrelevant at best. Two prominent finance theories gave rise to this perspective. Under Modigliani and Miller's (1958) perfect capital market assumptions, a firm's value does not depend on its capital structure, which by implication makes risk management irrelevant. Furthermore, the capital asset pricing model (CAPM) [Sharpe, 1964; Lintner, 1965] implies that investors care only about systematic risk. This stream of finance theory relies heavily on the distinction between systematic risk and firm-specific risk. According to CAPM theory, an investor can efficiently and inexpensively diversify away firm-specific risks until only systematic risk remains, which implies that risk management activities by the firm are not value enhancing.

Whereas the Modigliani and Miller model and CAPM assume perfect capital markets, various frictions exist in actual capital markets as well as in the many non-capital markets that firms operate in, potentially allowing firm-specific risks to impose real costs on firms. These frictions include taxes (Mayers and Smith, 1982; Smith and Stulz, 1985), asymmetric information costs (Myers and Majluf, 1984; Froot *et al.*, 1993), financial distress costs (Mayers and Smith, 1982; Smith and Stulz, 1985), underinvestment costs (Myers, 1977; Mayers and Smith, 1987; and Bessembinder, 1991), payments to non-diversifiable stakeholders (Mayers and Smith, 1990; Stulz, 1996), and agency costs. Due to these frictions, firm-specific risk management that reduces variability in performance could theoretically increase firm value. Some empirical studies find a positive relation between financial risk management and firm value. For example, Allayannis and Weston (2001) find that firms using foreign currency derivatives have on average almost a five percent higher firm value than non-users. Other studies have questioned these results. For example, Jin and Jorion (2006) investigate oil and gas firms and find no evidence that firms using derivatives to hedge their oil and gas risk increase firm value relative to firms that do not hedge. In general, risk management research in finance has narrowly focused on risk for which quantitative data is readily available, such as risk transfer using derivatives to transfer financial risk and insurance to transfer hazard risk.

Work has also started on operational risk management where the tools used are different from those used for hazard and financial risks. Operational risks are not typically normally distributed, exhibiting positive skewness with fat tails, and suffer from lack of data as losses are relatively infrequent and unique to the company. Cowell *et al.* (2007) argue that operational risks are difficult to evaluate using traditional econometric models. They discuss various tools that may be useful for modelling operational risk, for example, system dynamics, neural networks, and fuzzy logic, which are nonparametric and nonlinear models. These authors also argue that operational risks are best handled by causal models rather than focusing on events (losses or consequences). Cowell *et al.* (2007) employ

Bayesian networks to investigate operational risks, which allows expert opinion input and regular updating to overcome the lack of data. Gatzert and Kolb (2014) describe work on modeling operational risk in the financial industry and develop a model for the insurance industry to look at the effects on premiums and capital requirements. For detailed coverage of risk management history, refer to Simkins and Ramirez (2008) and Kloman (2010).

3. Traditional risk management (TRM) in practice

Despite the intense debate about the effectiveness, and even the relevance of corporate risk management among finance scholars, the practice has grown and evolved over the past six decades. This section describes the history of risk management as it developed in three corporate silos: insurance management, financial risk management, and internal control/audit.

The original corporate risk management was known as "insurance management", and mainly involved buying insurance to transfer hazard risks. Starting in the mid-1950s, a few academics, drawing on the work of Henri Fayol and practitioners promoted a broader view and the term "risk management" (Gallagher, 1956; Kloman, 1992). In 1963, two professors published the first risk management textbook (Mehr and Hedges, 1963). This textbook proposed the risk management process that is still familiar today (D'Arcy and Brogan, 2001). In words that anticipate ERM, the textbook also proposed that all risks should be managed comprehensively to "maximize the productive efficiency of the enterprise". However, risk management that followed in practice focused on measurable risks siloed by corporate departments. Decades passed before the ERM philosophy gained traction.

Also in 1963, Doug Barlow at Massey Ferguson became the first person at a company to receive the title of "risk manager". Barlow introduced the "cost of risk" concept in 1966, which included risk management costs beyond risk transfer (insurance), such as costs related to risk avoidance, risk mitigation, and risk retention (Kloman, 1992). In 1975, the American Society of Insurance Management (ASIM) changed its name to the Risk and Insurance Management Society (RIMS) to emphasize that members applied a risk management process, which involves more than just purchasing insurance to transfer risk, but involves a process to proactively manage risk rather than just financing after the loss occurs. Until the late 1970s, corporate risk management mainly aimed to reduce losses related to pure risks, which are insurable risks, including property damage, product liability, workers' compensation, and business interruption, and some types of operational risks, such as worker safety, but largely ignored potential losses related to financial risks, where gain is also possible.

A second corporate risk management silo arose when sophisticated financial risk management became practical with the development of the Black-Scholes options-pricing model in the mid-1970s. The option pricing model gave practitioners an analytical tool to price options. This model underlays the massive growth in the derivatives industry, which allowed the hedging of financial risk, such as currency, interest rate, commodity price, and credit risks. Firms often use derivatives to hedge financial risks along with insurance and other practices to manage pure risks without coordinating these activities. Firms managed risk in silos where corporate risk managers focused on

insurable risks (and related operational activities), and the treasury department managed financial risks, often using capital structure and derivatives.

A third risk management silo emerged with the entry of the accounting profession via internal control/audit and is largely compliance focused. Prompted by financial scandals in the late 1980s and early 1990s, various commissions started to redefine the mission of internal control to include risk management and corporate governance roles for internal auditors (Spira and Page, 2003; Huber and Rothstein, 2013). For example, the COSO Internal Control—Integrated Framework (1992) proposed that the internal control process should provide assurance that the firm complies with laws and regulations and provides reliable financial reporting. In COSO (1992), risk assessment assumes an important role for what is generally compliance based risk management. Various commissions and task forces have been influential in the development of risk management (Simkins and Ramirez (2008); Kloman (2010)). The Cadbury Report (Cadbury, 1992) suggests that the board of directors is responsible for the risk management policy to ensure the enterprise makes efforts to become aware of major risks. In 1994 in response to major bankruptcies, the Dey Report recommended that the Toronto Stock Exchange require listed companies to identify and understand major risks facing the corporation. In 1995, Canadian Institute of Chartered Accountants released the Criteria of Control (CoCo) model, which considers risk management in the achievement of an organization's objectives. The Hampel Report, Committee of Corporate Governance (Hampel, 1998) states that directors are responsible for control issues with the duty to set up a risk management system capable of identifying, assessing, and managing major risks to the enterprise. The Turnbull Report, Combined Code (Turnbull, 1999) advocates a key role for internal control in monitoring the effectiveness of the risk management system. During the 1990s, proposals are made for internal control/audit to take a broader risk management and corporate governance role. In 1999, the Institute of Internal Auditors (IIA) officially adopted a new definition of "internal auditors" that includes risk management and governance roles (Ramamoorti, 2003).

> Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

In addition to the three silos mentioned above, risk management dwells in other silos, such as supply chain research, which has traditionally focused on making the supply chain more efficient. Leaner supply chains are often more vulnerable to disruption, and thus less resilient, which has led to an increasing focus on supply chain risk management (Stecke and Kumar, 2009), but the research "ignores or does not seem aware of the wider literature on risk" (Khan and Burnes, 2007). The term "ERM" is not commonly used in supply chain research, but the work being done by scholars on the collaborative risk management necessary among firms in strategic supply chain relationships (see for example, Hallikas, Puumalainen, Vesterinen, and Virolainen, 2005) should become of interest to researchers in other disciplines. In a supply chain consisting of multiple firms, collaboration among firms reduces some risks but may introduce other risks. ERM advocates a portfolio view of the risks facing an individual firm. This work moves risk management beyond individual firms to a portfolio view of the risks jointly faced by multiple firms. Additionally, the term "strategic risk management" (SRM) has become widely used leading to confusion

about the relationship between SRM and ERM (Bromiley *et al.*, 2016). Is SRM a separate silo from ERM? If ERM encompasses the entire portfolio of risks faced by an organization, why is SRM being considered separately from ERM?

The risk management mantle worn by these siloed communities of interest inside corporations has caused much confusion in the evolution and implementation of enterprise-wide risk management. ERM is promoted as integrated, holistic risk management, yet practice and research is still siloed. Within companies, multiple functions, such as insurance/risk management, treasury, internal audit, and managerial accounting are locked in turf battles over the ERM mantle. An understanding of the origins and development of ERM out of these corporate silos is essential to promoting collaboration across disciplines, which is necessary for the ERM philosophy to be realized. Increasingly, executives have recognized the need to move away from silos toward a more encompassing risk management process. Integrated risk management can reduce overall risk at lower cost than efforts to address each risk independently (Miller, 1992). A task force representing multiple disciplines published AS/NZS 4360: 1995, which is the first risk management standard with updates in 1999 and 2004, and became the basis for ISO 31000: 2009 (Kloman, 2010). Over time, the disadvantages of the traditional silo view of risk management in an increasingly complex and interconnected world became manifest and the evolution toward ERM began.

4. What is enterprise risk management (ERM)?

Regulators, rating agencies, business publications, firms, and academics have reacted to spectacular corporate scandals and business failures over the last twenty years with an increased focus on risk management. In response, an evolution away from silo risk management began in the mid-1990s. ERM proposes the integrated management of all risks facing an organization as well as the alignment of risk management with corporate governance and the overall corporate strategy (Ramirez and Simkins, 2008). A tremendous volume of ERM articles have appeared in the business press, but academic work is still in an introductory and fragmented state. For an overview of ERM research by RMI and accounting scholars, see Bhimani (2009), Iyer *et al.* (2010), McShane *et al.* (2011), Soin and Collier (2013), Lundqvist (2014), and Gatzert and Martin (2015).

After almost two decades, ERM appears to be an aspiration rather than a reality as evidenced by the failure during the 2008 financial crisis of major corporations that professed to have implemented advanced ERM. It can be argued that the ERM philosophy is flawed or that organizations have not implemented ERM effectively or a combination of the two. Power (2005) classifies ERM as a "boundary object" that crosses multiple interests. Incorrect implementation could be due to confusion about ERM, which has evolved out of multiple academic, professional, and departmental silos that have not yet been integrated. Bromiley *et al.* (2015) provide tables of more than 25 definitions/descriptions of ERM found in the academic and industry literature between 1996 and 2011. The author considers the ERM philosophy to be sound, but that implementation has been problematic and proposes application of organizational design science to alleviate implementation difficulties.

The resulting confusion is evident. Definitions and descriptions indicate the fluidity of the ERM concept, which has been termed a "new paradigm/paradigm change", "emerging paradigm", or "paradigm shift" in risk management (Selim and McNamee, 1999; Barton *et al.*, 2002; Beasley *et al.*, 2005; Silvestri *et al.*, 2011); a "truly holistic, integrated, forward looking and process-oriented approach" (Deloach, 2000); a "systematic and integrated approach" (Dickinson, 2001); a "strategic business discipline" (Risk and Insurance Management Society (RIMS, 2011); a "process" (Committee of Sponsoring Organizations (COSO, 2004); an "evolution of risk management" (Fraser *et al.*, 2008); and an "evolving discipline" (Mikes and Kaplan, 2014). Descriptions in Power (2007) further illustrate the ambiguous nature of the ERM concept: "umbrella concept", "should not assume that ERM refers unequivocally to a coherent set of practices", "mixed bag of reformist, organizing sensibilities", "a new way for talking about control in organizations", "a discourse which envisages the integration of control and organizational strategy", and "an umbrella for a world-level organizational model".

With regulatory pressure on firms to integrate risk management into corporate governance, new risk categories and definitions have been created leading to the "risk management of everything" (Power, 2004), which Power (2009) ultimately concludes has resulted in the "risk management of nothing". Various types of ERM have been described. Power (2005) and Mikes (2005 and 2009) describe multiple strands of ERM that have evolved out of traditional risk management. ERM practice and academic research is still in a contentious beginning stage with multiple competing frameworks, such as COSO (2004) and ISO 31000 (2009), being debated within multiple, but siloed disciplines (Mikes, 2005; Purdy, 2010). The transition from narrow traditional risk management (TRM) to holistic ERM largely remains an ideal with poorly integrated implementation and disparate practices grouped under the same label (Arena *et al.*, 2010).

A broad search of the literature is summarized in Table 1 to distinguish traditional risk management (TRM) from enterprise risk management (ERM),

Table I.

Characteristics of traditional vs enterprise risk management

Place Table Here

5. Accounting research contributions to ERM

Case studies, qualitative work, and multidisciplinary collaboration have been a legitimate method of academic enquiry in accounting journals for decades (Hopper and Bui, 2016). Accounting researchers have drawn on work from other disciplines to advance ERM research. The ERM philosophy includes governance and management control concepts that are difficult to investigate solely using statistical and deductive methods. These aspects of ERM are difficult to quantify using relative frequency probabilities, which in essence is a reference-class problem (McGoun, 1995). Accounting scholars have broadened ERM research by embedding with risk management professionals to perform field studies. These academics are attempting to become more connected to practice by understanding what risk management professionals are actually doing in the context of their enterprises with the goal of "integrating theory and generalizable conceptual frameworks with skilled practice" (Kaplan, 2011).

The complex topic of ERM and its relationship to internal control, internal audit, and corporate governance requires a wide range of research methodologies, such as field research and contingency theory. Contingency theory has been employed to explain findings in various case studies of the effect of enterprise context and choice of management control and risk management systems. Application of field research and contingency theory is an important step to broaden research on risk management and provide a deeper understanding beyond narrow financial perspectives. In a field study taking a contingency perspective, Mikes (2009) finds varying calculative cultures among enterprises that shapes the adoption of ERM practices to fit risk management control to organizational contexts. Woods (2009) employs a case study method to understand the contingency variables for risk control system implementation in public sector organizations. Wahlström (2009) surveys employees dealing with regulation in four banks and finds that views toward risk management are contingent on organizational structure. Using a case study method, Jordan *et al.* (2013) find that risk maps are used to "adjudicate interests" among "distributed actors" in addition to producing early warning signals and audit trails as a defensive measure to avoid blame. They find risk maps being used as mediating devices employed to overcome boundaries and gain commitment between diverse groups across enterprises.

Tekathen and Dechow (2013) perform a case study that documents the difficulties and unintended consequences of mechanistically cascading objectives and responsibilities for risk through an enterprise and aggregating risk data from risk owners into a consolidated view. The study calls into question the COSO ERM view that ERM is similar to accounting with the capability of information being decomposed and recombined as it flows in a hierarchy. ERM catalogs uncertainty, which does not add up like the objects of accounting. This work reinforces the problem of internal control/audit based ERM argued by Power (2004 and 2009).

In practice, the internal control/audit function is assuming a prominent role in enterprise risk management for many organizations. In relation to risk management, a main goal of internal audit is to "provide objective assurance to the board on the effectiveness of risk management " (IIA, 2009). However, internal audit has been found in practice to be going beyond this core assurance role (Arena *et al.,* 2011) into execution of the risk management function, which

can be of serious concern to the independence and objectivity of internal audit (de Zwaan *et al.*, 2011). Among accounting professionals, it's logical that management accountants are suitable to be involved in the "management" role of ERM, not the internal audit function whose role should be compliance and independent assessment of the effectiveness of ERM. Too strong involvement by internal control/audit leads to ERM that is tick-the-box compliance oriented instead of a strategic partner in risk-adjusted decision making.

While cases of effective ERM implementation have been documented (see for example, Fraser and Simkins (2010), Fraser *et al*. (2015) and Aabo *et al*. (2005)), most firms struggle with turf battles and complexities associated with breaking down corporate silos, which is necessary for successful ERM implementation. IEC/FDIS 31010 (2009), Quail (2012), and Fraser and Simkins (2016) describe various tools/techniques that have been found useful for implementing ERM, such as ERM policies and frameworks, executive risk committees, risk champions, risk criteria, risk registers, and key risk indicators. In addition, performing risk assessments to allocate capital based on risks is useful for various constituencies to come to an agreement about why and how many resources are needed to mitigate risks to meeting objectives (Toneguzzo, 2010).

6. Application of organizational design science to ERM implementation

A few authors have advocated the application of systems thinking to the ERM process (O'Donnell, 2005; Pinto *et al.*, 2012; Bharathy and McShane, 2014; Lee and Green, 2015). Collopy (2009) argues that in theory, systems thinking should be beneficial to organizations but that in practice "the number and sequence of things that must be done has become so arcane that to master it seems all but impossible". Organizational design science is more accessible since a main tenant is to take small steps and make improvements by learning from mistakes. The complete system does not have to be understood before moving forward. The design science approach can be applied to bridge practice and theory in the area of change management by considering "management as design" and thoroughly understanding direct participants (Mohrman, 2007).

Design science has origins in the work of Simon (1969) who distinguished between the sciences of the natural and artificial, and Schön's (1983) discussion of the sciences of the artificial with a focus on using design methods to solve field problems. A goal of design science is to "focus on desired outcomes" and "interactions between researchers and practitioners", not "solving pure knowledge problems" (van Aken, 2007). After encountering a disconnect between theory based on research and actual practice, some Organizational Development scholars recommended design based research (DBR) to narrow the gap using a participatory approach to iteratively create knowledge suitable to a particular organization attempting to make significant changes (Andriessen, 2007). With the goal of improving professional practice, these researchers design interventions, test them in actual organizations, then iteratively modify interventions based on learning from the results. This DBR approach leads to heuristics that can be prescribed to solve real-world problems.

This paper proposes an organizational design science approach for effective ERM implementation. Design science is not geared toward a search for the truth and explanation, but focuses on solutions to field problems that involves iteration between synthesis, evaluation, and redesign in which empathy with directly involved stakeholders is crucial. This approach is suitable for implementing changes in an organization, which are not amenable to one-size-fits-all solutions. Change management is difficult due to the complex interconnectedness of modern organizations. Implementing ERM effectively involves breaking down functional silos, which typically faces substantial resistance from players comfortable in the silos. Design science handles this difficulty by tinkering and learning in small steps. In design with a learning focus, the initial design is just a starting point with regular tweaking and redesign as learning occurs.

Organizations attempting a radical change from traditional risk management to the ERM paradigm will face strong resistance from most employees who are naturally resistant to new concepts that involve substantial change (Mohrman, 2007; Fraser and Simkins, 2016). Johnson (2007) discusses the differences between real option reasoning (ROR) and path dependency theory in managing uncertainty. This manuscript views organization design science as following a real options philosophy to break path dependency and facilitate organizational change necessary to implement ERM. Design thinking is empathetic to those resisting change and makes the adjustment more palatable by taking small steps with learning that allows necessary course changes in the evolution toward ERM.

Building on Garud *et al.* (2007), this paper argues that applying real options reasoning implicit in design science allows a break from path dependence and a move toward path creation in which employees from various functional groups can use improvisation and bricolage to navigate through an uncertain implementation process. In discussing complex adaptive systems and emergence, Stacey (2007) questions the concept of a "system", which implies closed boundaries, and recommends that empathy for actors' experiences needs to be understood via brainstorming and experimentation. These arguments correspond to the organizational design science philosophy.

Even with two prominent ERM frameworks (COSO ERM and ISO 31000), organizational contexts make a one-size--fits-all method of implementing ERM impossible. Applying organizational design science to implement ERM does not involve following a plan completely mapped out in advance, but uses trial and error with learning gained and applied after each step to move forward pragmatically instead of painstakingly gathering data before acting. Organizational design science relies on participatory co-design by members who will be essential for organizational change to be successful (Bate and Robert, 2007). The author specifically proposes applying a design science approach to the ISO 31000: 2009 risk management process. ISO 31000 is accepted globally as a risk management standard. Associated with the standard is ISO 73:2009, which is a vocabulary guide. With various disciplines being involved in risk management, a standard accepted vocabulary is essential to reduce miscommunication.

Organizational design science is an iterative approach in which adjustments can be made in response to evolving conditions because options are kept open and exercised when beneficial. Applying the approach can produce an

agile ERM process resulting in a dynamic capability that allows a firm to thrive in a rapidly changing environment (Nair *et al.*, 2014; Bogodistov and Wohlgemuth, 2017). For design science, experimenting is essential and making mistakes is socially and psychologically safe, not considered to be failure but as learning opportunities. Design science can build an enduring capacity for change that enables continuous adaptation with ERM becoming an experimental learning-by-doing process.

Buchanan (2004) advocates an "interaction design" approach to facilitate relationships and capture the diverse expertise that exists in an organization. Boundary objects can be used to bridge the gap between different knowledge communities to increase the likelihood of effective change management initiatives (Romme and Damen, 2007). Boundary objectives, such as iterative prototyping, have long been applied for designing products, but can also be applied to organizational change interventions (Coughlan *et al.*, 2007). In a risk management case study, Jordan *et al.* (2013) investigate the use of risk maps as boundary objectives to mediate interests of diverse actors distributed across functional boundaries. Design problems require experimentation and the use of boundary objects to blend thinking and acting to transcend the gulf between academic and pragmatic perspectives and facilitate collaboration (Romme and Damen, 2007). The pragmatic emphasis of organizational design science is on creating actionable knowledge aimed at solving problems.

To become resilient in the face of an uncertain future, organizations must develop the capability to continually adapt to rapidly changing circumstances. Extending design science beyond the development of products and services, organizations can change by empathetically understanding participants, applying brainstorming techniques to generate possible solutions, prototyping rapidly to test potential solutions, learning from the prototyping, then honing in on the most effective solutions. Fraser and Simkins (2016) emphasize that ERM has to be acknowledged as a change management initiative and propose several techniques for implementing ERM, such as performing pilots first, then expanding as learning takes places. Quail (2010) and Fraser (2010) describe risk workshops and risk interviews that involve brainstorming and much more to facilitate cross-disciplinary cooperation across the enterprise. Prototyping bridges theory and practice by allowing progress from the abstract to the concrete with experimental trial and error and a bias toward action rather than extensive planning and analysis. Prototyping serves as a boundary object that catalyzes communication and permits integration of multiple viewpoints, resulting in participatory co-design. Failing early and often is tolerated as the key to learning and moving forward. The goal is to test ideas quickly and inexpensively and learn from the results. Failure after investing too much in time and resources to test an idea can be embarrassing, often leading to doubling down instead of making necessary course corrections. Small changes that are reversible before being set in stone allow rapid learning and effective collaboration by disparate participants that cannot be achieved by extensive analysis.

7. Conclusions and future research

Advancement of enterprise risk management (ERM) research and practice has been hampered by a complex evolution involving fragmented disciplinary treatment, competing professional associations and standards, and

siloed corporate risk management functions. To reduce confusion about ERM, this paper provides a history of risk management research and practice resulting in a table describing the basic differences between ERM and traditional risk management (TRM). With this foundation, this paper summarizes the contributions of accounting scholars moving beyond the limited potential of quantitative analysis by conducting field studies to understand what enterprises are actually doing. The paper also documents the contribution of scholars from other disciplines, such as management and systems engineering.

Over the previous few decades, various types of risk and uncertainty have been described that do not yield to disciplinary solutions and are often made worse. Broad, complex problems cannot be effectively handled by a single profession or discipline. Much of the academic work on ERM first came from finance then an essential expansion from accounting scholars with some work starting in other disciplines. Future research will require creativity and concerted interdisciplinary efforts for the holistic ERM philosophy to become effective. Collaboration among scholars from multiple disciplines is essential for the advancement of ERM.

The author also proposes effective ERM implementation as the next frontier for research collaboration across disciplines. Change management is difficult in a complex social system, such as an organization. With competing interests protecting turf and rapidly changing circumstances contingent on individual organizations, no generally proscribed method is possible for implementation of ERM in organizations. This paper proposes organizational design science as a way to deal with these difficulties. In contrast to explanatory sciences, a main emphasis of design science is to solve field problems, such as change management initiatives. Implementing ERM is a change management issue that defies typical planning procedures. Long-term planning is difficult in the face of uncertainly where locking in decisions can take an enterprise further down the wrong path. In a complex, interconnected world in which change is continuous, an organizational design science perspective can provide the foundation to implement effective ERM resulting in sustainable organizations. Organizational design science includes gaining knowledge on the fly that is essential to implementing the design.

Researchers following the path described in this work might be interested in proposing a framework for the application of a design science approach to implementing the ISO 31000: 2009 risk management process and developing a case to illustrate the usefulness of the approach. For example, referring to the Purdy (2010) description below of ISO 31000, a potential case could focus on the Communication and Consultation and Monitor and Review areas, which are parts of the process that require continuous updating and adjustments and buy in from diverse stakeholders, and thus where a design science approach is likely to be most effective.

- "Communication and consultation with internal and external stakeholders, where practicable, to gain their input to the process and their ownership of the outputs. It is also important to understand stakeholders' objectives, so that their involvement can be planned and their views can be taken into account in setting risk criteria.
- Monitoring and review, so that appropriate action occurs as new risks emerge and existing risks change as a result of changes in either the organization's objectives or the internal and external environment in which they are pursued. This involves environmental scanning by risk owners, control assurance, taking on board

new information that becomes available, and learning lessons about risks and controls from the analysis of successes and failures."

Good design that is conducive to allowing a diverse group of participants achieve their goals is important for successful implementation of change management initiatives. A design mindset allows sense making for those participants that need to be brought on board for organizational change. A design science approach is suitable to build the capacity for organizational change that is necessary for implementing effective ERM, which is not one-size fits all but depends on the contextual factors of the specific company.

References

Aabo, T., Fraser, J. R., and Simkins, B. J. (2005), "The rise and evolution of the chief risk officer: enterprise risk management at Hydro One", *Journal of Applied Corporate Finance*, Vol. 17 No. 3, pp. 62-75.

Ai, J., Brockett, P. L., Cooper, W. W. and Golden, L. L. (2012), "Enterprise risk management through strategic allocation of capital", *Journal of Risk and Insurance*, Vol. 79 No. 1, pp. 29-56.

Allayannis, G. and Weston, J. P. (2001), "The use of foreign currency derivatives and firm market value", *Review of Financial Studies,* Vol. 14 No. 1, pp. 243-276.

Andersen, T. and Schrøder, P. (2010), *Strategic Risk Management Practice,* Cambridge University Press, Cambridge, UK.

Andriessen, D. (2007), "Designing and testing an OD intervention reporting intellectual capital to develop organizations", *The Journal of Applied Behavioral Science*, Vol. 43 No. 1, pp. 89-107.

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

Arena, M., Arnaboldi, M., and Azzone, G. (2011), "Is enterprise risk management real?", *Journal of Risk Research*, Vol. 14 No. 7, pp. 779-797.

Barton, T. L., Shenkir, W. G. and Walker, P. L. (2002), *Making Enterprise Risk Management Pay Off: How Leading Companies Implement Risk Management,* Financial Times-Prentice Hall, Upper Saddle River, NJ.

Bate, P. and Robert, G. (2007), "Toward more user-centric OD lessons from the field of experience-based design and a case study", *The Journal of Applied Behavioral Science*, Vol. 43 No. 1, pp. 41-66.

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

Beasley, M. and Frigo, M. (2010), "ERM and its role in strategic planning and strategy execution", in Fraser, J.R. and Simkins, B. J. (Eds), *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*, John Wiley & Sons, Inc., Hoboken, New Jersey, pp. 31-50.

Bessembinder, H. (1991), "Forward contracts and firm value: investment incentive and contracting effects", *The Journal of Financial and Quantitative Analysis,* Vol. 26 No. 4, pp. 519-532.

Bharathy, G. and McShane, M. (2014), "Applying a systems model to enterprise risk management", *Engineering Management Journal,* Vol. 24 No. 4, pp 38-46.

Bhimani, A. (2009), "Risk management, corporate governance and management accounting: emerging interdependencies", *Management Accounting Research*, Vol. 20 No. 1, pp. 2-5.

BIS (2003), "Trends in risk management and aggregation", Bank for International Settlements (BIS) Joint Forum, available at: http://www.bis.org/publ/joint07.pdf (accessed 3 March 2017)

Bogodistov, Y. and Wohlgemuth, V. (2017), "Enterprise risk management: a capability-based perspective", *Journal of Risk Finance*, Vol. 18 No. 3, in press.

Branson, B. (2010), "The role of the board of directors and senior management in enterprise risk management", in Fraser, J.R. and Simkins B. J. (Eds.), *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives,* John Wiley & Sons, Inc., Hoboken, New Jersey, pp. 51-67.

Bromiley, P., McShane, M., Nair, A. and Rustambekov, E. (2015), Enterprise Risk Management: Review, Critique and Research Directions, *Long Range Planning*, Vol. 48 No. 4, pp. 265-276.

Bromiley, P., Rau, D. and McShane, M. (2016), "Can strategic risk management contribute to enterprise risk management? A strategic management perspective", in Andersen, T. J. (Ed), *Routledge Companion on Strategic Risk Management*, Routledge, New York, NY, pp. 140-156.

Buchanan, R. (2004), "Management and design: interaction pathways in organizational life", in Boland, R. and Collopy, F. (Eds.), *Managing as Designing,* Stanford University Press, Palo Alto, CA, pp. 55-63.

Cadbury, 1992, The Financial Aspects of Corporate Governance, available at: http://www.ecgi.org/codes/documents/cadbury.pdf (accessed 10 July 2016)

Collopy, F. (2009), "Lessons learned–why the failure of systems thinking should inform the future of design thinking?", available at: http://www.fastcompany.com/1291598/lessons-learned-why-failure-systems-thinking-should-inform-future-design-thinking (accessed 3 March 2017)

COSO (1992), "Internal control—integrated framework", Committee of Sponsoring Organizations of the Treadway Commission", available at: http://www.sox-online.com/coso-cobit-center/original-coso-framework/ (accessed 3 March 2017)

COSO (2004), "Enterprise risk management–integrated framework", Committee of Sponsoring Organizations of the Treadway Commission, available at: http://www.theiia.org/media/files/virtual-seminars/COSO_ERM_Integrated_Framework.pdf (accessed 3 March 2017)

Coughlan, P., Suri, J. F. and Canales, K. (2007), "Prototypes as (design) tools for behavioral and organizational change a design-based approach to help organizations change work behaviors", *The Journal of Applied Behavioral Science*, Vol. 43 No. 1, pp. 122-134.

Cowell, R. G., Verrall, R. J. and Yoon, Y. K. (2007), Modeling operational risk with Bayesian networks", *Journal of Risk and Insurance*, Vol. 74 No. 4, pp. 795-827.

D'Arcy, S. P. and Brogan, J. C. (2001), "Enterprise risk management", J*ournal of Risk Management of Korea*, Vol. 12 No. 1, pp. 207-228.

Deloach, J. (2000), *Enterprise-Wide Risk Management: Strategies for Linking Risk and Opportunity*, Financial Times/Prentice-Hall, London.

de Zwaan, L., Stewart, J. and Subramaniam, N. (2011), "Internal audit involvement in enterprise risk management", *Managerial Auditing Journal*, Vol. 26 No. 7, pp. 586-604.

Dickinson, G. (2001), "Enterprise risk management: its origins and conceptual foundations", T*he Geneva Papers on Risk and Insurance-Issues and Practice*, Vol. 26 No. 3, pp. 360-366.

Fraser, J.R., Schoening-Thiessen, K. and Simkins, B. J. (2008), "Who reads what most often? A survey of enterprise risk management literature read by risk executives.", *Journal of Applied Finance*, Vol. 18 No. 1, pp. 73-91.

Fraser, J.R. (2010), "How to prepare a risk profile", in Fraser, J.R. and Simkins, B.J. (Eds), *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*, John Wiley & Sons, Inc., Hoboken, New Jersey, pp.171-188.

Fraser, J.R. and Simkins, B. J. (2010), Enterprise risk management: Today's leading research and best practices for tomorrow's executives, John Wiley & Sons, Inc., Hoboken, New Jersey.

Fraser, J.R., Simkins, B. J. and Narvaez, K. (2015), Implementing enterprise risk management: Case studies and sest practices, John Wiley & Sons, Inc., Hoboken, New Jersey.

Fraser, J.R. and Simkins, B.J. (2016), "The challenges of and solutions for implementing enterprise risk management", *Business Horizons*, Vol 59 No. 6, pp.689-698.

Froot, K. A., Scharfstein, D. S. and Stein, J. C. (1993), "Risk management: coordinating corporate investment and financing policies", *The Journal of Finance,* Vol. 48 No. 5, pp. 1629-1658.

Gallagher, R. B. (1956), "Risk management: a new phase of cost control", *Harvard Business Review,* Vol. 34 No. 5, pp. 75-86.

Garside, T. and Nakada, P. (2000), "Enhancing risk measurement capabilities", *Balance Sheet,* Vol. 8 No. 3, pp.12-17.

Garud, R., Kumaraswamy, A. and Karnøe, P. (2010), "Path dependence or path creation?", *Journal of Management Studies*, Vol. 47 No. 4, pp.760-774.

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

Gatzert, N., and Kolb A., 2014, Risk Measurement and Management of Operational Risk in Insurance Companies from an Enterprise Perspective, *Journal of Risk and Insurance,* Vol. 81 No. 3, pp. 683-708.

Gatzert, N. and Martin, M. (2015), "Determinants and value of enterprise risk management: empirical evidence from the literature", *Risk Management and Insurance Review*, Vol. 18 No. 1, pp. 29-53.

Hallikas, J., Puumalainen, K., Vesterinen, T., and Virolainen, V. M. (2005), "Risk-based classification of supplier relationships", *Journal of Purchasing and Supply Management*, Vol 11 No. 2, pp. 72-82.

Hampel, 1998, Committee on Corporate Governance, available at: http://www.ecgi.org/codes/documents/hampel_index.htm (accessed 10 July 2016)

Harrington, S. E., Niehaus, G. and Risko, K. J. (2002), "Enterprise risk management: the case of United Grain Growers", *Journal of Applied Corporate Finance*, Vol. 14 No. 4, pp. 71-81.

Hopper, T. and Bui, B. (2016), "Has management accounting research been critical?", *Management Accounting Research*, Vol. 31, pp. 10-30.

Huber, M. and Rothstein, H. (2013), "The risk organisation: or how organisations reconcile themselves to failure", *Journal of Risk Research*, Vol. 16 No. 6, pp. 651-675.

IEC/FDIS 31010 (2009), "Risk management — Risk assessment techniques", available at: http://ehss.moe.gov.ir/getattachment/f7de1f2a-7559-49b5-8b97-c69b13fa17a9/ (accessed 22 June 2017)

IFAC (1999), "Enhancing shareholder wealth by better managing business risk", International Federation Of Accountants: PriceWaterhouseCoopers, available at: http://devbiz.narod.ru/home/kozloff/PWC/risk_mngmnt99.pdf (accessed 3 March 2017)

IIA (2009), "IIA position paper: the role of internal auditing in enterprise-wide risk management", available at: https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Role%20of%20Internal%20Auditing%20in%20Enterprise%20Risk%20Management.pdf (accessed 3 March 2017)

ISO 31000 (2009), "Risk management – principles and guidelines", available at: http://www.iso.org/iso/home/standards/iso31000.htm (accessed 3 March 2017)

Iyer, S.R., Rogers, D.A.,and Simkins, B.J. (2010), "Academic Research on Enterprise Risk Management", in Fraser, J.R and Simkins, B. J. (Eds), *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*, John Wiley & Sons, Inc., Hoboken, New Jersey, pp. 419-439.

Jin, Y. and Jorion, P. (2006), "Value and hedging: evidence from U.S. oil and gas producers", *The Journal of Finance,* Vol. 61 No. 2, pp. 893-919.

Johnson, W.H.A. (2007), "Managing uncertainty in innovation: the applicability of both real options and path dependency theory", *Creativity and Innovation Management*, Vol. 16 No. 3, pp 274-281.

Jordan, S., Jørgensen, L. and Mitterhofer, H. (2013), "Performing risk and the project: risk maps as mediating instruments", *Management Accounting Research*, Vol. 24 No. 2, pp. 156-174.

Kaplan, R. S. (2011), "Accounting scholarship that advances professional knowledge and practice", *The Accounting Review*, Vol. 86 No. 2, pp. 367-383.

Khan, O. and Burnes, B. (2007), "Risk and supply chain management: creating a research agenda", *The International Journal of Logistics Management*, Vol. 18 No. 2, pp.197-216.

Kloman, F. (1992), "Rethinking risk management", *The Geneva Papers on Risk and Insurance-Issues and Practice*, Vol. 17 No. 3, pp. 299-313.

Kloman, F. (2010), "A Brief History of Risk Management", in Fraser, J.R. and Simkins, B. J. (Eds), *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*, John Wiley & Sons, Inc., Hoboken, New Jersey, pp. 19-29.

Lee, L. S. and Green, E. (2015), "Systems thinking and its implications in enterprise risk management", *Journal of Information Systems*, Vol. 29 No. 2, pp. 195-210.

Lintner, J. (1965), "The valuation of risk assets and the selection of risky investments in stock portfolios and capital budgets", *The Review of Economics and Statistics,* Vol. 47 No. 1, pp. 13-37.

Lundqvist, S. A. (2014), "An exploratory study of enterprise risk management: pillars of ERM", *Journal of Accounting, Auditing & Finance*, Vol. 29 No. 3, pp. 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*, Vol. 34, pp. 441-466.

Marks, N. (2015), *World-Class Risk Management*, CreateSpace Independent Publishing Platform, Lexington, KY.

Mayers, D. and Smith Jr, C. (1982), "On the corporate demand for insurance", *Journal of Business*, Vol. 55, pp. 281-296.

Mayers, D. and Smith Jr, C. (1987), "Corporate insurance and the underinvestment problem", *Journal of Risk and Insurance*, Vol. 54, pp. 45-54.

Mayers, D. and Smith Jr, C. (1990), "On the corporate demand for insurance: evidence from the reinsurance market", *Journal of Business*, Vol. 63, pp. 19-40.

McCrae, M. and Balthazor, L. (2000), "Integrating risk management into corporate governance: the Turnbull guidance", *Risk Management*, Vol. 2 No. 3, pp. 35-45.

McGoun, E. G. (1995), "The history of risk measurement", *Critical Perspectives on Accounting*, Vol. 6 No. 6, pp. 511-532.

McShane, M., Nair, A., Rustambekov, E., 2011, "Does enterprise risk management increase firm value?", *Journal of Accounting, Auditing & Finance,* Vol. 26 No. 4, pp. 641-658.

Mehr, R. and Hedges R. (1963), *Risk Management in the Business Enterprise*, Richard D. Irwin, Inc., Homewood, IL.

Miccolis, J. (2002), "The language of enterprise risk management: a practical glossary and discussion of relevant terms, concepts, models, and measures", Tillinghast-Towers Perrin, available at: http://www.irmi.com/expert/articles/2002/miccolis05.aspx (accessed 3 March 2017)

Mikes, A. (2005), "Enterprise risk management in action", Centre for the Analysis of Risk and Regulation (CARR), Discussion Paper No. 35., available at:

http://www.lse.ac.uk/accounting/CARR/pdf/DPs/Disspaper35.pdf (accessed 3 March 2017)
Mikes, A. (2009), "Risk management and calculative cultures", *Management Accounting Research*, Vol. 20 No. 1, pp. 18–40.
Mikes, A. (2011), "From counting risk to making risk count: Boundary-work in risk management", *Accounting, Organizations and Society*, Vol. 36 No. 4, pp. 226-245.
Mikes, A. and Kaplan, R. S. (2014), "Managing risks: towards a contingency theory of enterprise risk management", working paper 13-063, Harvard Business School, 13 January.
Mikes, A. and Kaplan, R. S. (2015), "When one size doesn't fit all: evolving directions in the research and practice of enterprise risk management", *Journal of Applied Corporate Finance*, Vol. 27, No. 1, pp. 37-41.
Miller, K. (1992), "A framework for integrated risk management in international business", *Journal of International Business Studies*, Vol. 23, pp. 311-331.
Modigliani, F. and Miller, M. H. (1958), "The cost of capital, corporation finance and the theory of investment", *The American Economic Review,* Vol. 48 No. 3, pp. 261-297.
Mohrman, S. A. (2007), "Having relevance and impact the benefits of integrating the perspectives of design science and organizational development", *The Journal of Applied Behavioral Science*, Vol. 43 No. 1, pp. 12-22.
Myers, S. (1977), "Determinants of capital borrowing", *Journal of Financial Economics,* Vol. 5 No. 2, pp. 147-175.
Myers, S. C. and Majluf, N. S. (1984), "Corporate financing and investment decisions when firms have information that investors do not have", *Journal of Financial Economics,* Vol. 13 No. 2, pp. 187-221.
Nair, A., Rustambekov, E., McShane and M., Fainshmidt, S. (2014), "Enterprise risk management as a dynamic capability", *Managerial and Decision Economics*, Vol. 35 No. 8, pp. 555–566.
Nocco, B. W. and Stulz, R. M. (2006), "Enterprise risk management: theory and practice", *Journal of Applied Corporate Finance*, Vol. 18 No. 4, pp. 8-20.
O'Donnell, E. (2005), "Enterprise risk management: A systems-thinking framework for the event identification phase", *International Journal of Accounting Information Systems*, Vol. 6 No. 3, pp. 177-195.
Pinto, A., McShane, M. and Bozkurt, I. (2012), "System of systems perspective on risk: towards a unified concept", *Int. J. System of Systems Engineering*, Vol. 3 No. 1, pp. 33–46.
Plessis, J., Schanfield, A. and Menevse, A. (2015), "JAA Inc.—a case study in creating value from uncertainty", in Fraser, J.R., Simkins, B. J. and Narvaez, K. (Eds.), *Implementing Risk Management: Case Studies and Best Practices*, John Wiley & Sons, Inc., Hoboken, New Jersey, pp. 427-459.
Power, M. K. (2004), *The Risk Management of Everything*, Demos, London.
Power, M .K. (2005), "The invention of operational risk", *Review of International Political Economy,* Vol. 12 No. 4, pp. 577-599.
Power, M. K. (2007), *Organized Uncertainty–Designing a World of Risk Management*, Oxford University Press, Oxford.
Power, M. K. (2009), "The risk management of nothing", *Accounting, Organizations and Society,* Vol. 34 No. 6-7, pp. 849-855.
Purdy, G. (2010), "ISO 31000: 2009—setting a new standard for risk management", *Risk Analysis*, Vol. 30 No. 6, pp. 881-886.
Purdy, G. (2011), "Risk Appetite–Is Using this Concept Worth the Risk?". *New Zealand: RiskPost*. available at: http://broadleaf.com.au/wp-content/uploads/2011/09/NZSRM_Risk-Appetite_Aug11_ver5.pdf (accessed 22 June 2017).
Quail, R. (2010), "How to plan and run a risk management workshop", in Fraser, J.R. and Simkins, B.J. (Eds), *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*, John Wiley & Sons, Inc., Hoboken, New Jersey, pp.155-170.
Quail, R. (2012), "Defining your taste for risk", *Corporate Risk Canada,* Spring, pp. 24-30.
Ramamoorti, S. (2003), "Internal auditing: history, evolution, and prospects", *The Institute of Internal Auditors Research Foundation*, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.464.2403&rep=rep1&type=pdf (accessed 3 March 2017)
RIMS (2011), "Why strategic management?", available at: https://www.rims.org/resources/ERM/Documents/FAQ%20on%20SRM%20and%20ERM%20FINAL%20April%2020%202011.pdf (accessed 3 March 2017)
Romme, A. G. L. and Damen, I. C. (2007), "Toward science-based design in organization development: codifying the process", *The Journal of Applied Behavioral Science*, Vol. 43 No. 1, pp. 108-121.
Schön, D. A. (1983), *The Reflective Practitioner.* Temple Smith, London.

Selim, G. and McNamee, D. (1999), "Risk management and internal auditing: what are the essential building blocks for a successful paradigm change?", *International Journal of Auditing*, Vol. 3 No. 2, pp. 147-155.
Sharpe, W. F. (1964), "Capital asset prices: a theory of market equilibrium under conditions of risk", *The Journal of Finance,* Vol. 19 No. 3, pp. 425-442.
Silvestri, A., Arena, M., Cagno, E., Trucco, P. and Azzone, G. (2011), "Enterprise risk management from theory to practice: the role of dynamic capabilities approach–the "Spring" Model", in D. Wu (Ed.), *Quantitative Financial Risk Management* (Vol. 3), Springer Verlag, Berlin Heidelberg, pp. 281-307.
Simkins, B. and Ramirez, S. A. (2008), "Enterprise-wide risk management and corporate governance", *Loyola University Chicago Law Journal,* 39(3), pp. 571-594
Simon, H. A. (1969), The Sciences of the Artificial, MIT Press, Cambridge, MA.
Smith, C. and Stulz, R. (1985), "The determinants of firms' hedging policies", *Journal of Financial and Quantitative Analysis,* Vol. 20 No. 4, pp. 391–405.
Sobel, P. J. and Reding, K. F. (2004), "Aligning corporate governance with enterprise risk management", *Management Accounting Quarterly*, Vol. 5 No. 2, pp. 29-37.
Soin, K. and Collier, P. (2013), "Risk and risk management in management accounting and control", *Management Accounting Research*, Vol. 24 No. 2, pp. 82-87.
Spira, L. F. and Page, M. (2003), "Risk management: the reinvention of internal control and the changing role of internal audit", *Accounting, Auditing & Accountability Journal*, Vol. 16 No. 4, pp. 640-661.
Stacey, R. D. *(*2007*), Strategic Management and Organisational Dynamics: The Challenge of Complexity*, Prentice Hall*:* Englewood Cliffs, NJ.
Stecke, K. E. and Kumar, S. (2009), "Sources of supply chain disruptions, factors that breed vulnerability, and mitigating strategies", *Journal of Marketing Channels,* Vol. 16 No. 3, pp 193-226.
Stroh, P. J. (2005), "Enterprise risk management at United Health Group", *Strategic Finance*, Vol. 87 No. 1, pp. 26-35.
Stulz, R. M. (1996), "Rethinking risk management", *Journal of Applied Corporate Finance,* Vol. 9 No. 3, pp. 8-25.
Tekathen, M. and Dechow, N. (2013), "Enterprise risk management and continuous re-alignment in the pursuit of accountability: a German case", *Management Accounting Research*, Vol. 24 No. 2, pp. 100-121.
Toneguzzo, J. (2010), "How to allocate resources based on risk", in Fraser, J.R. and Simkins, B.J. (Eds), *Enterprise Risk Management: Today's Leading Research and Best Practices for Tomorrow's Executives*, John Wiley & Sons, Inc., Hoboken, New Jersey, pp.189-217.
Turnbull (1999), "Internal control: guidance for directors on the Combined Code", available at: http://www.ecgi.org/codes/documents/turnbul.pdf (accessed 3 March 2017)
Van Aken, J. E. (2007), "Design science and organization development interventions aligning business and humanistic values", *The Journal of Applied Behavioral Science*, Vol. 43 No. 1, pp. 67-88.
Wahlström, G. (2009), "Risk management versus operational action: Basel II in a Swedish context", *Management Accounting Research*, Vol. 20 No. 1, pp. 53-68.
Woods, M. (2009), "A contingency theory perspective on the risk management control system within Birmingham City Council", *Management Accounting Research*, Vol. 20 No. 1, pp. 69-81.

Table I.
Characteristics of traditional vs enterprise risk management

Traditional Risk Management (TRM)	Enterprise Risk Management (ERM)*
View: Silo view of risk. Deals with risks independently. No systematic understanding of interdependencies and correlation among risks.	View: Portfolio view of risk. Deals with risks holistically. Interdependencies and correlation among risks analyzed and understood. Natural hedges recognized and exploited. Understands internal/external contexts in evaluating risk portfolio.
See Harrington *et al.* (2002); Power (2005); Ai *et al.* (2012); and Lundqvist (2014).	
Limited strategic scope or influence. Technical and tactical not strategic. RM not an important element in decision making by board of directors and top management and not considered important in corporate governance. Middle management function.	Considers the entity's risk appetite/criteria in evaluating strategic alternatives for achieving objectives. Board of directors and CEO are strongly involved with ERM, which plays an important role in corporate governance. Risk management is an essential consideration in strategic decisions.
See Turnbull (1999); McRae and Balthazor (2000); COSO (2004); Sobel and Reding (2004); Mikes (2005); Stroh (2005); Arena *et al.* (2010); Beasley and Frigo (2010); Branson (2010); Andersen and Schrøder (2010); Purdy (2011); Ai *et al.* (2012); Lundqvist (2014 and 2015); and Marks (2015).	
No consideration for the allocation of capital.	Economic capital view: allocating capital to achieve the highest risk-adjusted return.
See Stulz (1996); IFAC (1999); Garside and Nakada (2000); Miccolis (2002); Power (2005); Sobel and Reding (2004); Mikes (2005); Nocco and Stulz (2006); Toneguzzo (2010); and Ai *et al.* (2012).	
Negative, cost based, and narrowly focused on downside only.	Positive, value based, broadly focused. Risk management is not only related to potential downside, but can be used to exploit opportunities to create value.
See Stulz (1996); IFAC (1999); Barton *et al.* (2002), and Plessis *et al.* (2015).	
Ambiguous ownership of some types of risk.	All risks assigned ownership with accountability.
See Power (2004); Nocco and Stulz (2006); and Power (2009).	
Focus is only on measurable risks, such as hazard and financial risks, while ill-defined operational or strategic risks, such as supply chain, cyber, and reputation risks may be acknowledged but ignored.	Adopts a single, comprehensive risk oversight structure and risk culture for dealing with all types of risk. Especially identifying and prioritizing top/critical risks and understanding root causes.
See Barton *et al.* (2002); Harrington *et al.* (2002); BIS (2003); Mikes (2005); Stroh (2005); Gates (2006); Ai *et al.* (2012); and Fraser and Simkins (2016)	