HARVARD | BUSINESS | SCHOOL

Towards a Contingency Theory of Enterprise Risk Management

Anette Mikes
Robert S. Kaplan

Working Paper

13-063

January 13, 2014

Towards a Contingency Theory of Enterprise Risk Management

Anette Mikes[1]

Harvard Business School

Robert S. Kaplan

Harvard Business School

January 13, 2014

[1] Corresponding author. Email: amikes@hbs.edu
We have received many helpful comments and suggestions from colleagues at HBS and elsewhere. We are particularly grateful to the discussants and session attendees at the AAA Congress in Anaheim in August 2013; the AAA Management Accounting Section conference in Orlando in January 2014, and to the participants of the accounting workshop at HEC Lausanne in November 2013.

TOWARDS A CONTINGENCY THEORY OF ENTERPRISE RISK MANAGEMENT

Abstract

Enterprise risk management (ERM) has become a crucial component of contemporary corporate governance reforms, with an abundance of principles, guidelines, and standards. This paper portrays ERM as an evolving discipline and presents empirical findings on its current state of maturity, as evidenced by a survey of the academic literature and by our own field research. Academics are increasingly examining the adoption and impact of ERM, but the studies are inconsistent and inconclusive, due, we believe, to an inadequate specification of how ERM is used in practice. Based on a ten-year field project, over 250 interviews with senior risk officers, and three detailed case studies, we put forward a contingency theory of ERM, identifying potential design parameters that can explain observable variation in the "ERM mix" adopted by organizations. We also add a new contingent variable: the type of risk that a specific ERM practice addresses. We outline a "minimum necessary contingency framework" (Otley 1980) that is sufficiently nuanced, while still empirically observable, that empirical researchers may, in due course, hypothesize about "fit" between contingent variables, such as risk types and the ERM mix, as well as about outcomes such as organizational effectiveness.

TOWARDS A CONTINGENCY THEORY OF ENTERPRISE RISK MANAGEMENT

An expanding list of companies, such as BP, Tokyo Electric, and Lehman Brothers, has become identified with failure to anticipate and manage risks within their organizations[2]. These examples of man-made disasters, along with many less catastrophic governance and corporate failures, reveal the challenges (and *in extremis*, to some, the futility) of enterprise risk management (ERM). While advocates argue that efficient risk management practices are the solution to the problem of how to avoid corporate disasters and failures (National Commission 2011), some skeptics see ERM as part of the problem itself (Power 2004; Power 2009). We have ample regulations and prescriptive frameworks for "enlightened" risk management, including the risk disclosure recommendations in the UK Turnbull report; the COSO Enterprise Risk Management Framework; and the International Standards Organisation's *ISO 31000:2009, Risk Management—Principles and Guidelines on Implementation*. More recently, the US Securities and Exchange Commission (SEC) has mandated that a publicly traded company's annual proxy statements include a description of the board's role in risk oversight. The Toronto Stock Exchange requires the establishment and disclosure of a company's risk management function, and the Dodd–Frank Wall Street Reform and Consumer Protection Act requires large publicly traded financial firms to have a separate board risk committee composed of independent directors. Credit-rating agencies now evaluate how firms manage risks, with Moody's and Standard & Poor's (S&P) having an explicit focus on ERM in the energy, financial services, and insurance industries (Moody's Analytics 2010; S&P 2013).

[2] Others on the list are Boeing, Bear Stearns, Merrill Lynch, Barings Bank, Daiwa Bank, Sumitomo, Enron, WorldCom, Tyco, and the Mirror Group.

With such an abundance of principles, guidelines, and standards, scholars might conclude that risk management is a mature discipline with proven unambiguous concepts and tools that need only regulations and compliance to be put into widespread practice. We disagree. We believe that risk management approaches are largely unproven and still emerging. Apparently, so do the many practitioners who have expressed dissatisfaction with the proposed normative and regulatory ERM frameworks (CFO Research Services and Towers Perrin 2008; Beasley, Branson, and Hancock 2010). We also believe that much academic research treats ERM as self-evident and fails to answer if its usefulness can be proven by more than its apparent popularity.

This paper begins with empirical findings on the current state of maturity of ERM as evidenced by a survey of academic research and by our own field research over the past decade. While many empirical papers have documented the prevalence and effectiveness of ERM, we believe that they have produced few significant results, largely because the perspective they employ uses an inadequate and incomplete specification of how ERM is implemented in practice. We propose—based on a ten-year field project, involving over 250 interviews with chief risk officers and three detailed case studies—a more comprehensive specification of ERM and identify the parameters that could serve as a solid foundation for a contingency theory of ERM design and implementation.

We studied three organizations with risk management practices that were actively supported and used by senior management. Yet each organization had a completely different structure and role for its risk management function. Based on this diversity of effective risk management systems, we conclude that it is too soon to predict which of these structures will survive to be incorporated into a future common body of knowledge for an emerging *risk management profession*. Prematurely adopting standards and guidelines that aspire to be

"applicable to all organizations" and "all types of risk" (as advocated, for example, by ISO 31000) introduces a major risk into risk management by inhibiting companies from searching for and experimenting with innovative risk management processes that match their particular circumstances. All three companies' solutions may be right—even optimal—for them; and other solutions may emerge for other company contexts. By adopting a contingency approach to ERM research, we avoid recommending a universal risk management system that should be applied in all circumstances. Instead, we search for the specific circumstances that would guide the selection of an appropriate risk management system for an individual enterprise.

1. Past Research on ERM Adoption and Performance

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) defined ERM as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives" (COSO 2004, 6).

This description evokes Anthony's widely quoted definition of management control: "the process by which managers assure that resources are obtained and used effectively and efficiently in the accomplishment of the organization's objectives" (Anthony 1965, 17). COSO advocates that ERM become a strategic management control system ("applied in strategy setting … to provide … assurance regarding the achievement of entity objectives"), just as the advocates of value-based management, activity-based management, the balanced scorecard, and other management control practices have preached. Unlike these other practices, however, ERM is not a measurement-centered practice. ERM focuses on "potential events" rather than on past performance and, therefore, has no uniquely identifiable measurement technology. Instead, ERM

users have produced, over the years, a variety of tools and processes to explicate future eventualities. In any particular company's ERM mix (Mikes 2009), one might find risk maps based on risk identification and assessment processes, stress tests based on data collection and statistical analysis, and scenario analyses based on scenario envisionment and planning.

Despite the plethora of risk management tools and processes, many organizations remain dissatisfied with existing risk management practices—their own and others'. In a September 2008 survey of CFOs (CFO Research Services and Towers Perrin 2008) about the causes of the global financial crisis, 62 percent of respondents blamed poor or lax risk management at financial institutions, ahead of the 59 percent who blamed financial instrument complexity, and the 57 percent who blamed speculation. Seventy-two percent of respondents expressed concern about their own companies' risk management practices. A majority of respondents in a survey of more than 400 leaders of ERM processes, including 20 percent from financial services (Beasley et al. 2010), reported dissatisfaction with their risk oversight processes; 42 percent described their risk oversight as "immature" or "minimally mature" and only three percent described theirs as "very mature."

Risk management's plethora of guidelines, frameworks, and tools has provided a tempting subject for academic research. Academic studies of ERM, have started to explore the dependence of ERM performance outcomes on organizational context, however, they fall short of putting forward a contingency theory of ERM. We have classified this literature into three categories, corresponding to three common concerns: selection studies, performance studies, and variation studies.

Selection Studies

In the first stream, the researchers attempt to use firm-specific contextual variables to explain the presence (or lack) of ERM. These studies mirror early contingency research in managerial and accounting research, which simply examined whether various plausible contingent factors (drivers) correlated with the control mechanism in question (Fisher, 1995). So the first thrust of empirical research on risk management was to identify the contextual factors related to ERM adoption. Based on the normative literature (COSO 2004; International Standards Organisation 2009), some studies verified the influence of boards and executive teams in securing ERM adoption (Beasley, Clune, and Hermanson 2005; Desender 2007), while others found the presence of an internal risk specialist to be associated with ERM adoption (Kleffner, Lee, and McGannon 2003; Beasley et al. 2005; Paape and Speklé 2012).

Another common observation is that firms carrying higher risk of financial distress (as measured by leverage or volatility of operating cash flows) are more likely than less-risky ones to adopt ERM (Liebenberg and Hoyt 2003; Pagach and Warr 2011). But empirical findings about some of the less-than-obvious contingency variables are mixed and even contradictory. Some studies identified *firm size* and *industry affiliation* as significant contingency factors (Colquitt, Hoyt, and Lee 1999; Beasley et al. 2005; Pagach and Warr 2011), while others found them non-explanatory (Liebenberg and Hoyt 2003*).* Studies of the impact of *institutional ownership* and *auditor influence* have yielded mixed results (Liebenberg and Hoyt 2003; Pagach and Warr 2011; Paape and Speklé 2012). As for *regulatory pressure*, Kleffner et al. (2003) reported that non-bank Canadian companies cited compliance with Toronto Stock Exchange guidelines as the third-most-important reason (37 percent) for their ERM adoption, confirming that nonfinancial firms also perceive external pressure to invest in ERM. Paape and Speklé (2012) found that stock

exchange listing was correlated with ERM implementation in Europe but found no association with the existence of *governance codes* or *risk management frameworks*.

Implicitly embracing the "survival of the fittest" principle, selection studies assume that only firms with effective combinations of context and ERM are observed, as those with an inappropriate combination will not survive. However, this form of Darwinism would apply only if ERM were indeed a mature discipline or if researchers could verify the continuing existence of the associations initially found in cross-sectional studies. Given the evolving nature of ERM, selection studies have identified few significant and design-relevant ERM variables and have so far ignored the process whereby organizations, over time, attempt to match their ERM to firm-specific contingencies. Nevertheless, these initial inquiries spurred the second stream of empirical studies that tried to assess whether ERM practices, on average, have contributed to better firm performance.

Performance Studies

A second stream of research seeks to identify the performance implications of ERM implementations (Pagach and Warr 2010; Pagach and Warr 2011; Beasley, Pagach, and Warr 2008; Hoyt and Liebenberg 2011; Ellul and Yerramilli 2012; Baxter, Bedard, Hoitash, and Yezegel 2012).

However, assertions about the value of ERM are not easy to establish in the face of a powerful financial economics paradigm that has, until very recently, been skeptical. From this perspective, shareholders can costlessly eliminate idiosyncratic risks through portfolio diversification so that any expenditure to establish and sustain a risk management function or to undertake risk-mitigating initiatives has a negative-net-present-value. Stulz (1996) argues,

however, that risk management adds value when it helps eliminate costly lower-tail earning outcomes. In other words, reducing the likelihood of performance shocks or the value destroyed during financial distress justifies ERM programs. Another finance theory argument (Froot, Scharfstein and Stein 1993) is that risk management adds value when it helps avoids states of the world in which the firm has insufficient internal funds to invest in positive-net-present-value opportunities.

In this spirit, researchers have performed stock exchange studies to observe whether financial markets attribute value to ERM implementation, but with mixed results.[3] The financial crisis of 2007-2008 offered a new testing ground for examining the effect of ERM on the performance of financial services firms. The results, again, were mixed and inconclusive.[4]

The inconclusive nature of these studies spurred a debate on method questions to explain conflicting results, and on the whole, distracted researchers from a deeper problem: namely that this literature is merely "controlling for" contingencies, rather than "theorizing" them. They appear to be working from the assumption that ERM is universally good or bad – which is inherently not in the spirit of contingency theories.

[3] Having studied a sample of financial and utilities firms over 1992-2004, and measured both stock-price reaction to announcements of ERM adoption and the effect of ERM on long-term performance, Pagach and Warr (2010; 2011) found no significant changes in various firm performance variables, which led them to conclude that ERM did not add observable value. Beasley et al. (2008), having studied the market reaction to 120 CRO announcements in the financial services, insurance, and energy sectors between 1992 and 2003, reported mixed results, suggesting that the costs and benefits of ERM must be firm-specific. Hoyt and Liebenberg (2011), however, did find a positive relation between ERM use and long-term firm value in a sample of insurers between 1998 and 2005.

[4] Having examined S&P ERM ratings for insurers and banks between 2006 and 2008, Baxter et al. (2013) concluded that better quality ERM did not lead to higher market performance prior or during the market collapse, while McShane, Nair, and Rustambekov (2010) contradicted this result and attested ERM's value added (at least for insurers over 2007-2008). In a recent, long-term study, Ellul and Yeramilli (2012) concluded that banks with a strong and independent risk function did indeed perform better during the financial crisis. Based on public data, they captured variation in the organizational structure and quality of risk-management functions, constructing their own "risk management index."

Most of these studies—with the exception of Ellul and Yeramilli (2012)—do not open the black box of ERM either, instead putting their faith in secondary assertions about the nature, maturity, and comparability of the practices that firms report under the ERM label. For instance, Liebenberg and Hoyt (2003), Beasley et al. (2008), and Pagach and Warr (2011) used the appointment of a chief risk officer (CRO) as a surrogate for ERM implementation. Beasley et al. (2005) measured the degree of ERM implementation with a simple scale ranging from "no plans exist to implement ERM" to "complete ERM is in place." Hoyt and Liebenberg (2011) identified ERM programs through Lexis-Nexis and SEC filings, while McShane et al. (2010) and Baxter et al. (2013) relied on S&P's ERM ratings.

Risk management practices taking place under a different label, such as those implemented by different staff functions or under the auspices of executives other than the CRO, have been excluded from these studies. But our main criticism is that many of the studies rely on simplistic variables to represent complex behavior. For example, the single 0-1 dummy variable of ERM adoption does not capture how ERM is actually implemented. Studies that rely on S&P's ERM ratings must assume that the rating agency's arm's-length assessment of a firm's ERM processes, based on public information, is a valid indicator of the risk management processes actually implemented in the firm. Because of these shortcomings, most empirical studies explain only a small fraction of the variability in the adoption or impact of risk management and have low statistical significance for key explanatory variables.

Further, the large-sample cross-sectional studies focus on the adoption of a particular risk management framework (for example, COSO's ERM) but ignore how the framework was implemented by the organization's leadership and employees. The effectiveness of risk management ultimately depends less on the guiding framework than on the people who set up,

coordinate, and contribute to risk management processes. It is people, not frameworks, that identify, analyze, and act on risk information. Their actions often require approval from the CEO and board. So the different organizational and cultural contexts in companies following the same ERM framework can lead to different implementation and use of risk management frameworks. For example, all Wall Street financial firms had risk management functions and CROs during the expansionary period of 2002-2006. But some of these firms failed in the subsequent crisis while others survived quite well. The existence of a risk management department and an individual with the title of chief risk officer explains very little about the quality, depth, breadth, and impact of a firm's risk management processes. For example, the fact that a company had a risk management department with a CRO does not predict that the department had the backing of the CEO and board to encourage the production and dissemination of risk information, nor that it had the resources, leadership, and support to mitigate the principal risks the risk department identified.

The essence of a contingency theory of ERM (beyond the simple selection / correlation studies) would be to find "fit" between contingent factors and firms' ERM practices, and to establish propositions of fit that will result in desired outcomes (for a review of contingency studies in management accounting, see for example Otley, 1980; Fisher, 1995; Chenhall, 2003, 2006). Moving towards a contingency theory of ERM requires a more sophisticated understanding of not only the nature of relevant contingencies, but also the nature of ERM itself.

There is now a growing strand of longitudinal field studies that tries to capture the fascinating variety of risk management practices in banking and elsewhere, deployed at different organizational levels, for different purposes, and by different staff groups—even by companies

in the same industry. Studies that can embrace such important variation may end up explaining more about ERM, especially about what works and what does not.

Variation Studies

The third and emerging stream of empirical work on ERM uses small-sample or field studies to understand risk management *in situ*, as an organizational and social practice, and has compiled sufficient evidence to suggest that risk management practices vary considerably across firms, even within an industry (Tufano 1996; Mikes 2009; Mikes 2011). In some firms, risk management takes the form of complex financial transactions (Tufano 1996; Chacko, Tufano, and Verter 2001); in others, it follows a more holistic assessment of financial and nonfinancial risks (Mikes 2009; Mikes 2011; Woods 2009; Arena, Arnaboldi, and Azzone 2010), bridging functional silos. Risk management in some firms consists only of policing the business for compliance with risk limits and risk policies while, in others, the function helps the organization learn about uncertainties in its strategy and in its external and competitive environment (Mikes 2009; Mikes, Hall, and Millo 2013; Power, Ashby, and Palermo, 2013).

This diversity provides an opportunity to develop grounded theories by studying actual risk practices in actual organizations. Such studies help us conceptualize and identify practices that may advance ERM, even when the company doesn't call them risk management or when they are performed outside the risk function. In the remainder of this paper, we draw on existing longitudinal field research and on several case studies, written between 2007 and 2012, in order to (1) provide a practice-based definition of ERM, (2) explicate the variables that cause the observed variation in ERM systems, and (3) propose contingency variables that explain some of

this variation, such as the nature and controllability of the firm's risks and the speed at which the firm's key uncertainties evolve.

A useful contingency theory must be more powerful than "it depends." The emerging theory should have an hypothesis about the specific linkages between organization-specific factors and the design of its ERM structure and systems, as well as a performance hypothesis about how improving the fit between an organization's specific factors and its ERM system design will improve its performance along specific, measurable dimensions.

2. Identifying Risk Management Processes

A former COSO chairman claimed (corresponding authors' interview with Larry Rittenberg) that any enterprise risk management approach should contain three components:

1. a strategic activity, addressing "potential events" that threaten the achievement of strategic objectives,

2. a governance activity, involving participation and oversight at multiple levels of management, and

3. a monitoring activity, based on the cybernetic control ideal of objective-setting (in the form of risk limits or risk appetite), measurement, feedback, and corrective action.

ERM systems with all three components, however, can still vary widely. Some firms may concentrate only on a narrow set of financial, insurable, or measurable events that threaten strategic objectives (Tufano 1996; Mikes 2009). Others address threats that encompass nonfinancial, qualitative issues as well (Mikes 2009; Woods 2009; Jordan, Jørgensen, and Mitterhofer 2013). As will be shown in our case studies, the unit of analysis for risk management

can vary—a project, an organizational subunit, or the entire firm—with each requiring a different degree of employee and managerial participation in the ERM process. Some firms are driven by a quantification-oriented calculative culture with a managerial predilection towards measurement and management by numbers (Mikes 2009), while others, more skeptical about the relevance and value of risk measures, emphasize the learning benefits from questioning and learning from the numbers (Mikes 2011). Finally, some organizations place more emphasis on risk measurement than others do simply because they *can*—their risks are more tangible and quantifiable.

The firms in our case studies deliberately introduced highly intrusive and interactive risk management processes to counter the individual and organizational biases that inhibit constructive thinking about risk exposures. Extensive psychological and sociological studies have documented biases (such as availability, confirmation, and anchoring) that cause individuals to grossly underestimate the range of possible outcomes from risky situations; people may be aware of various risks, but they grossly underestimate the adverse consequences from their occurrence (Hammond, Keeney, and Raiffa 2006; Kahneman, Lovallo, and Sibony 2011). Often, managers and employees, especially under budget and time pressure, become so inured to particular risks that they override existing controls and accept deviances and near misses as the "new normal"—a behavior referred to as the normalization of deviance (Vaughan 1999). By treating red flags as false alarms rather than as early warnings of imminent danger, they incubate more vulnerability to risk events. Firms also make the mistake of "staying on course" when they shouldn't. As events begin to deviate from expectations, managers instinctively escalate their commitment to their prior beliefs, "throw good money after bad," and incubate even more risk.

In addition to these individual biases, organizational biases, such as "groupthink," also inhibit good thinking about risks. Groupthink arises when individuals, still in doubt about a

course of action that the majority has approved, decide to keep quiet and go along. Groupthink is especially likely when the group is led by an overbearing, overconfident manager who wants to minimize conflict, delay, and challenges to his or her authority.

All these individual and group decision-making biases explain why so many organizations overlook or misread ambiguous threats and fail to foresee how bad things can happen to their good strategies.

Based on these considerations and on the characteristics of emerging ERM practices, we propose the following practice-based definition of ERM:

Enterprise risk management consists of active and intrusive processes that (1) are capable of challenging existing assumptions about the world within and outside the organization; (2) communicate risk information with the use of distinct tools (such as risk maps, stress tests, and scenarios); (3) collectively address gaps in the control of risks that other control functions (such as internal audit and other boundary controls) leave unaddressed; and, in doing so, (4) complement—but do not displace—existing management control practices.

3. Three Studies of Mature ERM Systems

For our case studies, we selected three companies in three industries—aerospace engineering, high-voltage electricity transmission, and fund management—and sought to uncover the explicit or implicit design choices they made for their risk management systems. The three companies' mature risk management systems had the following characteristics:

- Longevity: it had been in existence for at least five years.
- Visible: it had the active support of top management.

- Interactive: not just checklists and compliance, it employed intrusive risk management tools and processes.
- Multi-functional: it encouraged the discussion of risks across functional silos and organizational boundaries.
- Actionable: it linked to the resource allocation process.
- Leadership: its head was a visible, senior officer, with a direct reporting line to the chief executive or other C-suite executive.

We conducted 38 interviews within the three companies between 2008 and 2012 (see Appendix 1 for a list of case-specific interviews and dates) and have been conducting ongoing email communications and follow-up visits to confirm that the risk management mix in each company has indeed reached the degree of maturity that makes it of interest for contingency research; that is, that we could ask and answer the question, "Why did these ERM systems take their specific—and differing—forms?"

Case 1. Aerotech

Aerotech, a research and development center, managed capital-intensive, time-critical technological projects for the US National Aeronautics and Space Administration (NASA) unmanned space missions. Despite some spectacular successes, Aerotech had had a mixed track record of managing risks. Its previous risk assurance function had focussed on checklists for quality control, which allowed many risks to incubate for a long time in functional silos only to emerge in unfortunate and rather spectacular failures.

In 2000, Aerotech hired a chief system engineer (CSE) to develop and implement a new risk management architecture that would significantly increase Aerotech's mission success rate.

The CSE knew that his principal challenge was to counter the overconfidence and biases of engineers about the riskiness of their projects:

> [Aerotech] engineers graduate from top schools at the top of their class. They are used to being right in their design and engineering decisions. I have to get them comfortable thinking about all the things that can go wrong. … Innovation—looking forward—is absolutely essential, but innovation needs to be balanced with reflecting backwards, learning from experience about what can go wrong.

The CSE introduced an independent and expert risk review board, which he chaired, to monitor the risks associated with each major project. The risk review board performed the following processes for every project:

1. A meeting with project engineers at the beginning of every project to review and challenge the engineers' assessment of the major risks.
2. Establish cost and time reserves, based on its assessments of the project's degree of innovation, to allow unforeseen problems to be solved during the course of the multiyear project without exceeding the project's budget or jeopardizing its scheduled launch date.
3. Annual or biannual three-day meetings with the project team where it vigorously challenges and debates the project team's current risk assessments.

The CSE also met quarterly with project leaders to update the risk assessments.

The rigorous monitoring and governance processes motivated engineers to build robustness and reliability into their everyday design decisions rather than ignoring potential problems or taking shortcuts to bypass them. The link from the risk monitoring activity to a

resource allocation activity (the cost and time reserves) gave the risk review board real power: it could reject or cancel projects that had inadequate funding to address the project's risks. As the project proceeded, the board could reallocate funds among project components and authorize disbursement from the cost reserves to employ tiger teams of outside experts to solve seemingly intractable design and engineering problems. As the launch date approached, the board recommended either that the launch proceed as planned or, if residual risks remained too high, that it be deferred. The built-in time reserves and the ultimate but costly deferral option reduced deadline pressures, an oft-cited cause of man-made disasters such as the *Challenger* launch decision and the explosion of the *Deepwater Horizon*'s drilling rig. The project that eventually led to the highly successful Mars landing of the rover, *Curiosity*, in August 2012 had actually been delayed two-and-a-half years because the project's risk review board recommended—only 45 days before the original launch date in 2009—that several technological risks remained too high.

Case 2. Electroworks

Electroworks, a major Canadian power utility, operated in an industry in which lack of reliability could lead not only to financial and asset damage but also to human injury and death. The provincial regulatory agency had capped the price that Electroworks could charge, while also requiring it to lead conservation initiatives that would reduce future revenues and earnings. Electroworks had to manage a complex web of conflicting interests—the agendas of government ministers, regulators, consumers, environmental groups, aboriginal (First Nation) landowners, and the capital-market debt-holders that had subscribed to the company's C$1 billion bond issue.

Its chief risk officer (CRO), originally hired from the banking industry to be the head of internal audit, had little domain expertise and was not an intrusive or hands-on risk manager. With no formal qualifications to challenge Electroworks' engineers at risk assessment workshops and at resource allocation meetings, the CRO functioned as a facilitator not a devil's advocate. His risk management department collected information about Electroworks' critical and material risks and distributed this information up, down, and across the enterprise. He established a "Chinese wall" to separate his internal audit role from his risk management one. Records of the risk workshops were kept confidential and separate from internal audit assessments and no one, besides himself, was involved in both activities. He had the strong backing of the CEO, who advocated a no-blame culture and encouraged people to speak up and report worrying deviances, issues, and potential threats.

Electroworks' CRO, along with a small team of risk managers, introduced a three-phase enterprise risk management program. In Phase 1, he organized a series of workshops at which employees collectively identified and quantified what they saw as the principal risks to the company's strategic objectives. These workshops used an anonymous voting technology that allowed employees to quantify, on a scale of 1 to 5, the impact of each risk discussed and its likelihood, having also assessed the strength of existing controls. These judgments were summarized into a risk map. Multiplying the likelihood and impact scores of each risk yielded a high-level ranking of the highest-priority risks to be mitigated. The risk map, albeit a simple and subjective tool, made it easier for people to discuss the proper focus of Electroworks' risk-mitigating actions.[5] Each meeting concluded with a consensus on the principal risks identified,

[5] Interestingly, the risk review workshops at Aerotech also used 5×5 risk maps to summarize the principal risks to the mission. While seemingly simplistic, especially for the PhD rocket scientists at Aerotech, the risk map's

the actions recommended to cost-efficiently mitigate each principal risk, and the manager who would be accountable for taking the recommended actions for each risk.

In Phase 2, the CRO conducted biannual one-on-one interviews with senior managers to review the corporate risk profile and then presented the results to the CEO and the board. In Phase 3, conducted during the annual planning process, the senior executive team allocated hundreds of millions of capital investment dollars among investment projects that had been proposed to mitigate the company's principal risks. By tying the investment management process to risk assessment, this ERM process gave business managers an incentive to disclose rather than hide risks, so that they could obtain resources to mitigate them. The mantra was, "If you have no risk, you get no money." The investment management department rigorously screened project proposals before they were presented at the two-day annual resource allocation meeting. Those meetings, like Aerotech's risk review board meetings, were intensively interactive as risk managers challenged the engineers' "bang for the buck" investment proposals.

All three phases channeled risk information vertically and horizontally throughout the company, enabling executives and employees to develop a shared understanding of what risks the company faced and what had to be done about them. Indeed, the CRO attributed the success of ERM to its multiple points of "contact" with employees:

> Enterprise risk management is a contact sport. Success comes from making contact with people. Magic occurs in risk workshops. People enjoy them. Some say, "I have always worried about this topic, and now I am less worried because I see that someone else is dealing with it, or I have learned it is a low-probability

plain summary of highly complex phenomena was enough to generate active discussion and debate during the meetings.

event." Other people said, "I could put forward my point and get people to agree that it is something we should be spending more time on, because it is a high risk."

In 2008, the CRO of Electroworks and his team initiated so-called "black swan workshops," a separate process to focus executives' and board members' attention on low-probability high-impact events that did not normally come up during risk workshops and face-to-face meetings with executives. These discussions used a new framework for brainstorming—a separate risk map that allowed the comparison and ranking of potential "black swan events" based on the velocity of the underlying trend and the company's perceived resilience to such events. He described the workshops to us as "more a thought experiment than a risk workshop." Not a regular part of the risk management calendar, they were held on demand (but at least annually), whenever the board saw the need to discuss a particular low-probability disaster that had yet to show up among in the periodic risk updates. Insights from the black swan workshops were fed back into the company's disaster recovery plans.

Case 3. Wealthfund

Wealthfund, a private-asset management bank within a very large money-center financial institution, offered investment opportunities to clients in external and internally-managed funds. It had an award-winning reputation for service and innovation in the global private banking business. Long-term client relationships, trust, and clients' private wealth were continually at stake and risk exposures changed frequently and rapidly. The bank's regulators, wary of its ample opportunities for self-dealing and conflicts of interest, required substantial due diligence on the external funds the bank offered its clients and even more on its internally- managed funds.

Regulators did not want investment managers directing client assets internally when there were better external options. Wealthfund's risk management function had to operate with independence and authority to approve the population of funds that asset managers could use and to ensure that all investment managers complied with external and internal requirements.

The focus of risk management between 2007 and 2010 was compliance with investment mandates across all teams and products despite market moves, liquidation requirements, and the portfolio managers' quest for gains in tumultuous markets. Risk managers also conducted an ongoing review of operational risks arising from breakdowns in documentation, clearing, and settlement or reporting. This was arguably more of an internal audit role, but there was a strong emphasis on the enforcement of controls aimed at risks that were liable to change in tumultuous markets.

After the onset of the global financial crisis, Wealthfund introduced another set of risk managers whose mandate was to work closely with managers within the business lines. Each "embedded" risk manager had dual reporting lines: one to the line manager and one to his or her own superior in the independent risk management function. One of the embedded risk managers explained the novelty of his dual responsibilities for improving the risk-adjusted returns for his managers' funds while protecting the portfolios from major downside shocks:

> My colleagues in independent [compliance] risk management who sit outside the [fund management] team don't necessarily have the proximity and real-time visibility of what trades and risks are being taken. So we want somebody on the inside looking out for everybody's interest and that person is me. I serve as a close business partner to portfolio managers … responsible for keeping portfolios

> in alignment with both broad private-bank-level policies … as well as [fund]-specific market-risk-related items such as trade approvals, portfolio risk analysis, positional concentrations, etc. … [M]y role is to keep portfolio managers honest … I listen to their views so I can help them fine-tune what they should sell and buy in order to reflect their views in their portfolios.

The embedded risk managers continually asked "what if" questions that forced portfolio managers to think about what different scenarios might mean for the private bank's performance. The risk managers challenged portfolio managers' assumptions and actions and helped them design trades prior to approval at investment committee meetings. To do this, they had to help portfolio managers assess how proposed trades contributed to the risk of the entire investment portfolio—not just under normal circumstances, but also under extreme stresses. For example, under conditions of market distress, the correlation of returns across different asset classes, such as stocks and bonds, increases dramatically. Stress-testing helped investment managers estimate potential extreme losses from low-probability events. One embedded risk manager explained that stress-testing made managers consider system effects and the unintended consequences of their planned actions:

> Portfolio managers come to me with three trades and the model may say all three trades are adding to the same type of risk. Nine times out of ten, a manager will say, "No, that's not what I was trying to do." Then we can sit down and redesign the trades.

Wealthfund's CEO reflected on the uncertainties highlighted by the recent financial crisis and their effect on the organization's approach to risk management:

> Things happened in 2008 that no one ever contemplated. The crisis catapulted risk managers to a seat at the management table. … The problem is not the known risks, it is the unknown risks. And for this you also need highly sophisticated, highly savvy people who have market skills and who can think about the "what ifs."

A strongly independent rules and compliance function (as Wealthfund's risk management originally was) can, over time, be seen as so independent and removed from business operations that line managers consider it of no help to them in coping with strategy-execution issues. Conversely, an embedded risk function, helping line managers address day-to-day risks, can "go native" and lose the independence required to maintain a strong compliance culture. Wealthfund's risk function strived to create a dual (or hybrid) structure to be both *independent overseer and business partner*.

4. Unpacking the "ERM Mix"

Our field studies (and others') illustrate different approaches and roles for the risk management function (Mikes 2009; Mikes, Hall and Millo, 2013; Power, Ashby and Palermo, 2013). Some act as the *independent overseer*, with an exclusive focus on compliance and internal controls. Others have moved beyond this to a *business partner* role. For example, Aerotech's risk management is embedded within the formal planning and resource allocation process and also influences key strategic decisions, such as approval or veto of new projects and whether to approve the actual launch of a mission. In the *independent facilitator* role, exemplified at Electroworks, risk management does not influence formal decision making but does acquire agenda-setting power and information with which to facilitate risk communication across the organization and the discussion of key strategic uncertainties. In the *dual or hybrid*

role, exemplified at Wealthfund, the risk function balances compliance with business orientation by deploying separate groups of independent and embedded risk managers.

The variety of ERM implementation seen in our three case studies, taken together with other field findings, also suggests that any observed "ERM mix" can and should be unpacked into a set of fundamental risk management components. These components (and their determinants) include:

Processes for identifying, assessing, and prioritizing risks. Risk identification can take place face-to-face (as in our three cases) or through self-assessments prompted remotely by a centralized database or risk register (Mikes, Tufano, Werker, and De Neve, 2009). Face-to-face meetings can be intensive, interactive meetings between the risk expert and the line managers, as practiced at Aerotech and Wealthfund, or open discussions among employees from different functions, and hierarchical levels, as practiced at Electroworks. Risk discussions can be confined to senior line managers and staff or can be decentralized by engaging front-line, support, and administrative staff as well. Further research is required to explicate contextual factors that may influence the shape of risk identification process: but based on contingency research on management control systems (Simons 2005), a number of organizational design parameters (span of control; span of accountability; span of influence and span of support), and the *interdependencies* in the task environment (Thompson, 1967) are likely to be relevant. For example, it was the reciprocal interdependencies across Aerotech's design teams that warranted wide span cross-silo risk discussions. At Electroworks and Wealthfund, where organizational and project units performed separate functions, the risk workshops were more focused on the project, department, business unit or portfolio at hand, and the range of participation in risk identification was determined by the diversity of functions involved in the management of these.

Frequency of risk meetings. Aerotech's project engineers had to make trade-offs between a mission's scientific goals and the immutable laws of physics. The risks associated with a particular mission were largely known by the end of the initial project meeting, and the laws of physics would not be changing during the course of the project. That helps to explain why formal updates on project risks could be adequately assessed at annual or biannual risk review meetings. In contrast, Electroworks's risks—from changes in demand, regulation, interest rates, and equipment—evolved continually, so it held risk workshops throughout the year, and led semiannual senior executive face-to-face risk assessments, and annual resource allocation meetings. Wealthfund's risks changed hourly, and even from one trade to the next, requiring continuous monitoring and assessment by embedded risk managers. We conclude from this variety that the frequency of risk identification and assessment processes must match the *velocity of risk evolution*, a bit of common sense that nevertheless tends to be lost in a "one size fits all," rules-based compliance framework.

Risk tools. Most companies use multidimensional visualizations, such as risk maps, to quantify risks along likelihood, impact, and controllability dimensions (Jordan et al. 2013). Electroworks and Aerotech conducted regular assessments and reviews of their high-level subjective rankings of their "top 10 risks." Companies, such as Wealthfund, with extensive historical data on asset pricing, covariance, and risk events go beyond simple risk map summaries by introducing data- and analysis-intensive statistical assessments, such as value-at-risk calculations and stress tests. We conclude from this variety that the choice of risk tools, ranging from qualitative descriptions and scenarios to the measurement of expected and unexpected loss, will be conditioned by (1) the availability of data and knowledge about a particular risk (loss) and (2) how relevant and reliable the available risk tools are in the eyes of

risk experts and everyone else using the tools.

Field research in financial services, where the raw data for risk analysis tends to be plentiful, suggests that the selection of particular risk tools tends to be associated with the firm's calculative culture—the measurable attitudes that senior decision makers display towards the use of sophisticated risk models (Mikes 2008; Mikes 2009; Mikes 2011). While some risk functions have a culture of *quantitative enthusiasm*, focusing on extensive risk measurement and risk-based performance management, others have a culture of *quantitative skepticism*, focusing instead on qualitative discourse and the mobilization of expert opinions about emerging risk issues.

How Risk Types Also Matter

Beyond dimensions related to the organizational context for risk management, Kaplan and Mikes (2012) introduced a taxonomy for classifying different types of risks events. Each of the taxonomy's three risk categories—preventable, strategy, and external—has a different source, a different degree of controllability, and a different approach for identification, mitigation, and management (see Table 1).

-------INSERT TABLE 1 AROUND HERE ----------

Preventable (Category I) risks arise from routine operational breakdowns or from employees' unauthorized, illegal, unethical, incorrect, or inappropriate actions. Companies gain nothing by tolerating such risks; they are inherently undesirable. Depending on the firm's tolerance for failure and on the existence of cost-effective controls, management should strive to reduce the incidence of preventable risks to zero.

In contrast, organizations voluntarily take on *strategy execution (Category II) risks* in order to generate superior returns. For example, some companies operate in inherently hazardous industries, such as mining, chemicals, and oil and gas exploration. Others, such as high-technology, pharmaceutical, medical device, and aerospace companies must engage in high-risk research projects to develop new products. Managers can influence both the likelihood and the impact of their strategy execution risks, but some residual strategy risk will always remain.

External (Category III) risks arise from events that the company cannot influence. Some of these risks are closely entwined with the firm's strategic choices and are therefore related to strategy execution risk. For example, mergers and acquisitions and geographical and market expansion entail the partly controllable risks of strategy execution, but they also introduce external uncontrollable uncertainties—new political, regulatory, and competitive environments—that are outside the firm's immediate control. Managers are often unaware of these external risks and, even when made aware, are unable to plausibly assess their likelihood. But that should not be the control objective for this category of risk. As external risks are, by definition, unavoidable and impossible to predict, the concern should be with the organization's resilience, should they occur. The assessment (and enhancement) of organizational resilience requires that the company introduce a process of risk envisionment—using experience, intuition, and imagination—to suggest plausible future disaster scenarios. Once a particular risk has been envisioned, managers can contemplate how the organization can respond—is their current resilience adequate to cope in the future, or does it need to be increased?

Organizations use different processes, departments, and actions for their different categories of risk events. Organizations that focus only on avoiding undesirable (Category I) risks, through compliance controls and compartmentalized risk management functional silos

(to address market, human resources, credit, and supply chain risks) leave themselves vulnerable to strategy execution and external risk events (Categories II and III). Neither rules-based compliance nor functional risk silos helped companies avoid disasters such as the global financial crisis, the BP *Deep Horizons* well explosion, and the developmental and operational problems of the new Boeing 787 Dreamliner aircraft.

While some risk management frameworks suggest that risk managers should focus mainly on preventable risks (as an enhancement of the internal audit process), others suggest that the ERM mix should focus mainly on strategy execution risks (COSO 2004; International Standards Organization 2009). We propose that risk management will be most effective when it matches *the inherent nature and controllability of the different types of risk* the organization faces. Our conclusion is that effective risk management "depends"; it is contingent on the organization's context and circumstances. We can offer preliminary ideas about what risk management likely depends *on*.

Towards a contingency framework for ERM

All three of our case studies explicitly addressed strategy execution risks. Aerotech's CSE believed that strategy risks are greatest when "the project's engineering enters territory we have never experienced before." He focused his new risk management processes on the risks from high innovation, leaving "business-as-usual risks" to internal controls and the existing quality assurance process. He stated, "we are familiar with those risks and know how to quantify and mitigate them."

Electroworks' risk function embraced a focus on strategy risks from the beginning. More recently, the CRO and his team initiated so-called "black swan workshops," a separate process to

envision uncontrollable, external (Category III) risks, and to check the organization's resilience to those risk events and the capabilities of its disaster management systems.

In contrast, Wealthfund's risk management department started off solely as an independent overseer (compliance function), which kept its risk managers isolated from the line business units. However, as the department's risk managers accumulated business-relevant expertise and as the line units began to request front-line risk management support, the department deployed embedded risk managers to address the rapidly-evolving strategy risks that emerged from volatile capital markets.

The only common characteristic in the three companies' risk management approaches was the use of highly interactive processes to address strategy execution risks, the risk review meetings at Aerotech, employee risk assessment meetings at Electroworks, and face-to-face interactions at Wealthfund. These intensive interactions provoked the dialogue and debate necessary to overcome biases (Hammond et al. 2006; Kahneman et al. 2011) that keep people from thinking rigorously about risks and bad outcomes. The meetings identified and assessed key strategy risks and helped managers select cost-efficient risk initiatives, something that cannot be achieved by filling out and auditing checklists or installing Governance, Risk, and Compliance (GRC) software.

All three companies, however, differed on their scope of their risk management function. Aerotech focused only on the risks from its strategic portfolio of unmanned space missions. Wealthfund's risk function managed both preventable and compliance risks as well as strategy risks, while Electroworks left preventable risks to its internal audit department, while its risk function managed strategy risks and, recently, board and senior executive deliberations about

external risks.

The three firms also had very different time cycles for their risk management processes. Aerotech performed its rigorous risk assessments annually or bi-annually; Electroworks conducted risk assessments throughout the year; and Wealthfund analyzed risk exposures minute by minute, even trade by trade.

As for the risk officers themselves, Aerotech's CSE and Wealthfund's CRO, facing high-risk technical problems, had deep domain expertise and the self-confidence to credibly challenge the assumptions or veto the decisions of highly expert and self-confident project engineers and investment managers. The Electroworks CRO dealt with an array of enterprise risks ranging from regulation, financing, and human resources to ice storms and aboriginal access rights. Since no individual could have expertise in these multiple domains, the CRO and his group facilitated information production and dissemination for decision making; they did not make or veto risk-based resource allocation decisions. For major investment decisions, the CRO collaborated with experts in the investment planning department—themselves former field and project engineers—to engage interactively and rigorously with current project engineers.

Table 2 summarizes the case comparisons and outlines the design parameters that differentiate the three ERM processes.

--------INSERT TABLE 2 AROUND HERE-------

Managing preventable (undesirable) risks should not be contingent on organizational structure and strategy. Proven tools and processes to manage preventable risks exist and their implementation can be standardized (see structural safeguards, system safeguards and staff safeguards in Simons, 2000: 284-288). In contrast, the tools for managing strategy and external

risks are still evolving and must vary with strategy-specific and firm-specific variables.

We have suggested several plausible and testable propositions about the fit between contingent variables, such as risk type (and other organizational or industry variables), and the ERM mix. We propose a framework (see Figure 1) that unpacks the ERM mix into its building blocks. It aligns specific ERM practices with the specific risk types they best address. This proposed matching—a "minimum necessary contingency framework" (Otley 1980)—enables empirical researchers to collect data and test hypotheses about "fit" and "outcomes" (organizational effectiveness). Although the measurement of organizational effectiveness will ultimately be the test of a contingency theory of ERM, the complexity of forces affecting organizational performance may initially call for the use of intervening variables as dependent variables in research studies. Initially, user satisfaction surveys and managerial perceptions of the ERM function are potential indicators of ERM effectiveness (Otley 1980), as is the very tenure and maturity of the risk management function, as we found in our cases.

-------–INSERT FIGURE 1 AROUND HERE----------

Given the evolving nature of risk control, it is unclear which of the tools and practices now in use will ultimately make up a "common body of knowledge" that can define the profession of enterprise risk management. Today, the job of identifying risks and helping business lines manage them falls not only to risk specialists, but also to internal auditors, strategic planners, finance staff, and management accountants (Rizzi, Simkins, and Schoening-Thiessen 2011; Grant Thornton Advisory Services 2012). ERM may indeed evolve into an "umbrella function" for the discussion of certain (or all) kinds of risk. Its advocates, the risk managers, may gain control of important organizational agendas, such as planning, resource

allocation, and reward systems and be able to standardize tools and reports that allow their companies to manage universal risk concerns. On the other hand, ERM may remain highly contingent on situational politics, opportunities, and demands, "plugging" the control gaps left unaddressed by other control agents. Either way, its success or failure depends on whether risk managers succeed in making their function both *seem* and *be* important to the control agents and processes already in place.

We encourage future research to refine our practice-based definition of risk management and to complete and operationalize the contingency variables we identified. With a sufficiently complete set of contingency building blocks, researchers will be able to better conceptualize "fit", along the lines of progress made in management accounting research (Burkert et al., 2013). In-depth, small sample, or longitudinal field studies should elicit a fascinating and revealing variety of context-specific practices and should, in due course, help us understand the causes and value of such variety. Over time, deductive and empirical researchers can hypothesize about and test the fit between ERM practices and different contexts. At that point, we can start codifying and standardizing a set of appropriate and *contingent* risk management practices.

APPENDIX 1 – LIST OF INTERVIEWS

Firm	Date	Interviewee
Aerotech	2008-10-08	Chief Systems Engineer
Aerotech	2009-02-26	Chief Systems Engineer
Aerotech	2009-06-05	Chief Systems Engineer
Aerotech	2009-08-07	Project Engineer
Aerotech	2009-08-10	Chief Systems Engineer
Aerotech	2009-08-10	Project Engineer
Aerotech	2012-03-01	Risk Review Board Member
Aerotech	2012-05-16	Risk Review Board Member
Aerotech	2012-05-29	Risk Review Board Member
Electroworks	2008-05-07	CFO
Electroworks	2008-05-07	CRO
Electroworks	2008-05-07	Risk Manager
Electroworks	2008-05-08	Manager
Electroworks	2008-05-08	Head of Investment Management
Electroworks	2008-05-08	Operations Manager

Electroworks	2008-05-08	CEO
Electroworks	2008-05-08	Director of Public Relations
Electroworks	2008-05-09	CRO
Electroworks	2008-05-09	Director of Regulatory Relations
Electroworks	2011-11-01	CRO, Senior Risk Manager #1
Electroworks	2011-11-01	CRO, Senior Risk Manager #2
Electroworks	2011-11-01	CRO, Senior Risk Manager #3
Electroworks	2011-11-01	Operations Manager
Electroworks	2011-11-01	Project Manager
Electroworks	2011-11-02	CRO, Senior Risk Manager #1
Firm	**Date**	**Interviewee**
Electroworks	2011-11-02	CRO, Senior Risk Manager #2
Electroworks	2011-11-02	Project Manager
Wealthfund	2008-06-20	Group CRO
Wealthfund	2008-06-08	Senior Manager
Wealthfund	2008-09-10	Group CRO
Wealthfund	2009-02-18	Group CRO

Wealthfund	2010-04-09	CRO (Embedded)
Wealthfund	2010-04-09	CRO (Business Unit)
Wealthfund	2010-04-09	Risk Manager (Independent)
Wealthfund	2010-04-09	Chief Investment Officer
Wealthfund	2010-05-12	Manager
Wealthfund	2010-05-12	CRO (Embedded)
Wealthfund	2010-05-12	Chief Investment Officer

APPENDIX 2 – TABLES AND FIGURES

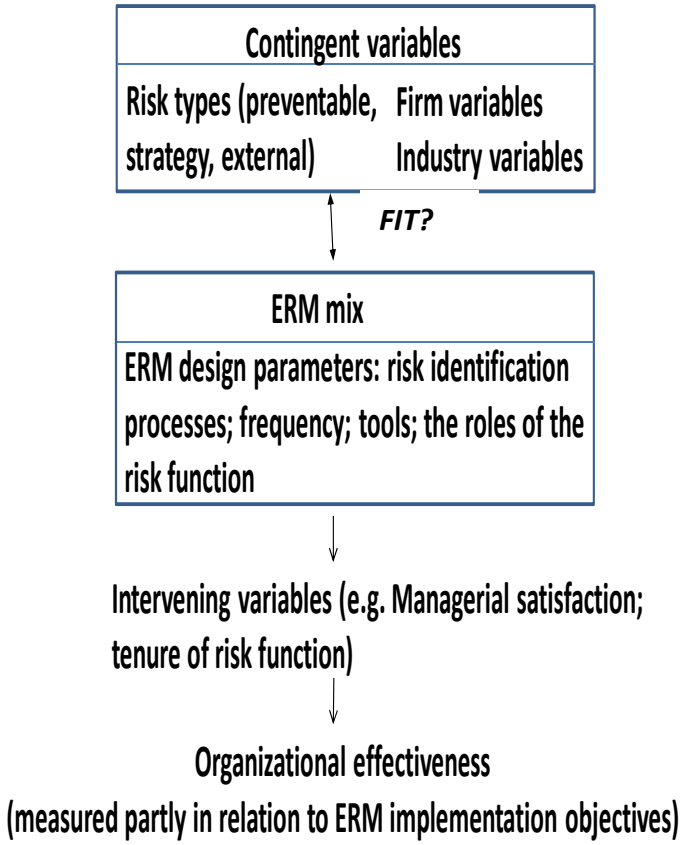
Table 1. Three Categories of Risk

Risk categories	Controllability and relationship to strategy	Control approaches
I. Preventable (undesirable) risks	Organizations may (in theory) prevent or cost-efficiently minimize occurrence of risk. There is no strategic benefit from taking these risks.	Internal control Boundary systems Mission and value statements Internal audit
II. Strategy execution risks	Organizations may reduce the likelihood and impact of such risks in cost-efficient ways. Taking these risks is essential for achieving strategic returns.	Risk identification with risk maps and registers Risk mitigation initiatives Risk monitoring linked to strategy review meetings and resource allocation
III. External risks	Organizations cannot control the occurrence of such risks, but may be able to prepare and thus reduce the impact.	Risk "envisionment" via scenarios, war games, and expertise-based mental models Contingency planning Insurance and hedging programs (limited use)

Table 2. Fundamental Components of ERM across the Three Cases

Design parameters: / Case:	**Processes for identifying risks**	**Frequency of risk identification**	**Risk communication tools**	**The risk function's role**
Aerotech	Risk review boards: independent and/or executive directors	Regular (annual or biannual)	Risk maps (impact and probability)	Business partner
Electroworks	Risk workshops: cross-functional groups at all staff levels; Face-to-face meetings (CRO and line management)	Both regular (twice a year) and on demand.	Risk maps (impact, control strength, and probability) Lists of top risks	Independent facilitator
Wealthfund	Face-to-face meetings (CRO and line management)	Regular (weekly)	Statistical "tail risk" and sensitivity analyses (what if)	Dual role: independent overseer and business partner

Figure 1. Minimum Necessary Contingency Framework for ERM



REFERENCES

Anthony, R.N. 1965. *Planning and Control Systems: A Framework for Analysis*. Boston, MA: Division of Research, Harvard Business School Publishing.

Arena, M., M. Arnaboldi, and G. Azzone. 2010. The organizational dynamics of enterprise risk management. *Accounting, Organizations and Society* 35 (7): 659–675.

Baxter, R., J.C. Bedard, R. Hoitash, and A. Yezegel. 2012. Enterprise risk management program quality: Determinants, value relevance, and the financial crisis. *Contemporary Accounting Research* Forthcoming.

Beasley, M.S., R. Clune, and D.R. Hermanson. 2005. Enterprise risk management: an empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy* 24 (6): 521–531.

Beasley, M., D. Pagach, and R. Warr. 2008. Information conveyed in hiring announcements of senior executives overseeing enterprise-wide risk management processes. *Journal of Accounting, Auditing and Finance* 28 (3): 311–332.

Beasley, M.S, B.C. Branson, and B.V. Hancock. 2010. Are you identifying your most significant risks? *Strategic Finance* 92 (5): 29–35.

Burkert, M., Davila, A., Mehta, K. and Oyon, D. 2013. Relating alternative forms of contingency fit to the appropriate methods to test them. *Management Accounting Research* 24 (4): xxx-xxx.

CFO Research Services, and Towers Perrin. 2008. *Senior Finance Executives on the Current Financial Turmoil*. Boston, MA: CFO Publishing Corp.

Chacko, G., P. Tufano, and G. Verter. 2001. Cephalon, Inc. taking risk management theory seriously. *Journal of Financial Economics* 60 (2-3): 449–485.

Chenhall, R.H. 2006. The contingent design of performance measures. In *Contemporary Issues in Management Accounting*, edited by Bhimani, A. 92–116. New York, NY: Oxford University Press, USA.

Chenhall, R.H. 2003. Management control systems design within its organizational context: Findings from contingency-based research and directions for the future. *Accounting, Organizations and Society* 28 (2): 127–168.

Colquitt, L.L., R.E. Hoyt, and R.B. Lee. 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 (COSO). 2004. *Enterprise risk management framework.* New York, NY: American Institute of Certified Public Accountants.

Desender, K. 2007. *On the determinants of enterprise risk management implementation*. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1025982.

Ellul, A., and V. Yerramilli. 2012. Stronger risk controls, lower risk: Evidence from U.S. bank holding companies. *Journal of Finance* 68 (5): 1757–1803.

Fisher, J. 1995. Contingency-Based Research On Management Control Systems: Categorization By Level Of Complexity. *Journal of Accounting Literature* 14 (1995): 24-53.

Froot, K. A., D.S. Scharfstein, and J. Stein. 1993. Risk management: Coordinating corporate investment and financing policies. *Journal of Finance* 48 (5): 1629–1658.

Grant Thornton Advisory Services. 2012. *Rising to new challenges: The view from the office of the CAE*. Available at: http://www.gt.com/staticfiles/GTCom/Advisory/Advisory%20publications/CAE%20survey/CAE-Survey- 2012_Executive_Summary.pdf, accessed January 2013.

Hammond, J. S., R.L. Keeney, and H. Raiffa. 2006. The hidden traps in decision making. *Harvard Business Review* 84 (1): 118–126.

Hoyt, R.E., and A.P. Liebenberg. 2011. The value of enterprise risk management. *The Journal of Risk and Insurance* 78 (4): 795–822.

International Standards Organisation (ISO). 2009. ISO 31000:2009, Risk Management—Principles and Guidelines. Geneva: International Standards Organisation.

Jordan, S., L. Jørgensen, and H. Mitterhofer. 2013. Performing risk and the project: Risk maps as mediating instruments. *Management Accounting Research* 24 (2): 156–174.

Kahneman, D., D. Lovallo, and O. Sibony. 2011. Before you make that big decision... *Harvard Business Review* 89 (6): 50–60.

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

Kleffner, A.E., R.B. Lee, and B. McGannon. 2003. The effect of corporate governance on the use of enterprise risk management: Evidence from Canada. *Risk Management and Insurance Review* 6 (1): 53–73.

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

McShane, M.K., A. Nair, and E. Rustambekov. 2011. Does enterprise risk management increase firm value? *Journal of Accounting, Auditing & Finance* 26 (4): 641–658.

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

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

Mikes, A. 2011. From counting risk to making risk count: Boundary-work in risk management. *Accounting, Organizations and Society* 36 (4-5): 226–245.

Mikes, A., M. Hall, and Y. Millo. 2013. How experts gain influence. *Harvard Business Review* 91, (7-8): 70–74.

Mikes, A, P. Tufano, E.D. Werker, and J-E. De Neve. 2009. The world food programme during the global food crisis (A). HBS No. 9-809-024. Boston, MA: Harvard Business School Publishing.

Moody's Analytics, Inc. 2010. *Enterprise Risk Management*. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CEgQF

jAA&url=http%3A%2F%2Fwww.moodysanalytics.com%2F~%2Fmedia%2FBrochures%2FAOE_Overview_Brochures%2FEnterprise-Risk-Solutions-Brochure.ashx&ei=90lUUvfNMIe14AOxsoDYCQ&usg=AFQjCNGmoXRIFOnbKl5CT5bOSfpVAXGIaA&sig2=_usdgQVbAzCOIneNXYtR1A&bvm=bv.53537100,d.dmg

National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling (National Commission). 2011. *Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling*. Report to the President. Available at: http://www.oilspillcommission.gov/final-report, accessed January 2013.

Otley, D.T. 1980. The contingency theory of management accounting: Achievement and prognosis. *Accounting, Organizations and Society* 5 (4): 413–428.

Paape, L., and R.F. Speklé. 2012. The adoption and design of enterprise risk management practices: An empirical study. *European Accounting Review* 21 (3): 533–564.

Pagach, D., and R. Warr. 2007. *An empirical investigation of the characteristics of firms adopting enterprise risk management*. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDEQFjAA&url=http%3A%2F%2Fpoole.ncsu.edu%2Fdocuments%2FRisk_officer_hazard_JBF.pdf&ei=ak1UUurNCdPD4AP0_4CoDQ&usg=AFQjCNH1KBQcBGu2JAQEMHOf0CfM6_mgXQ&sig2=1_9oegbACW1ADu0NbmiD2w&bvm=bv.53537100,d.dmg

Pagach, D., and R. Warr. 2010. *The effects of enterprise risk management on firm performance*. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1155218.

Pagach, D., and R. Warr. 2011. The Characteristics of Firms that Hire Chief Risk Officers. *The Journal of Risk and Insurance* 78(1): 185–211.

Power, M. 2004. *The risk management of everything: Rethinking the politics of uncertainty*. London, UK: Demos.

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

Power, M., Ashby, S., & Palermo, T. 2013. *Risk Culture in Financial Organisations*. London, UK: Research Report for London School of Economics, Centre for the Analysis of Risk and Regulation.

Rizzi, J., B.J. Simkins, and K. Schoening-Thiessen. 2011. *Enterprise Risk Management: A Review of Prevalent Practices.* Ottawa: Conference Board of Canada.

Simons, R. 2000. *Performance Measurement and Control Systems for Implementing Strategy*. Prentice Hall..

Simons, R. 2005. *Levers of Organization Design*. Boston, MA: Harvard Business Review Press.

Standard & Poor's Financial Services LLC. 2013. *Ratings Direct: Criteria, insurance, general: Enterprise risk management*. New York, NY: McGraw-Hill. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CE8QFjAB&url=http%3A%2F%2Fwww.standardandpoors.com%2Fspf%2Fupload%2FRatings_US%2FEnterprise_Risk_Management_5_7_13.pdf&ei=gkhUUuWPKrbK4AOs5IHQCQ&usg=AFQjCNGZDFgzHS6rapcAkCCqA_cPu0g-Mw&sig2=DUiif0dOed12MLMBfktvhA&bvm=bv.53537100,d.dmg

Stulz, R. 1996. Rethinking risk management. *Journal of Applied Corporate Finance* 9 (3): 8–24.

Thompson, J.D. 1967. *Organizations in Action.* Transaction Publishers: New Brunswick (U.S.A.) and London (U.K.)

Tufano, P. 1996. Who manages risk? An empirical examination of risk management practices in the gold mining industry. *Journal of Finance* 51 (4): 1097–1137.

Vaughan, D. 1999. The dark side of organizations: Mistakes, misconduct, and disaster. *Annual Review of Sociology* 25 (1): 271–305.

Woods, M. 2009. A contingency theory perspective on the risk management control system within Birmingham City Council. *Management Accounting Research* 20 (1): 68–91.