The Biggest Gap in ERM Practice:
The Human Element and the Science of Risk

James Bone

Abstract

Enterprise risk management frameworks (such as, COSO ERM, ISO 31000, and NIST's Cybersecurity guidance) have one thing in common – each of the traditional risk frameworks are based on guidance for establishing rudimentary foundations for the development of risk management programs. Along the way, the term "guidance" has been confused or substituted with "standard(s)" of risk practice and in many cases (especially for early adopters) is assumed to be the summation of a mature risk management program. The challenge traditional risk frameworks face is that the "E" in enterprise risk management is no longer applicable as the world transitions to Industry 4.0 and hybrid models of business and military operations. Technology has extended the walls of the enterprise to the cloud and a variety of third-party and tertiary vendors who do not maintain the same standards as self-contained organizations. Secondarily, but more importantly, none of the traditional risk frameworks include scientific rigor found in Prospect Theory, Decision Science, Behavioral Science, Cognitive Science, or the lesser sciences of Human Factor Analysis. The existing gaps in traditional risk frameworks expose organizations to greater risks at the same time of increasing technological complexity, higher rates of cyber threats and advancements in artificial intelligence which creates an inflection point in corporate governance writ large. This article proposes the need for additional rigor in traditional risk guidance or wholesale revisions to the concept of risk management practice in corporate governance.

In the wake of successive corporate financial fraud, Sarbanes-Oxley of 2002 required "independent auditors" of public companies must report to an audit committee which generally include, at least one "financial expert". Nevertheless, the audit committee alone cannot anticipate or respond to all the risks facing a contemporary organization. "It seems axiomatic that today the public corporation too often fails to identify and manage the risks [it] faces" (Ramirez & Simkins, 2008) historically leading to a lack of confidence in corporate risk management functions.

(The following are excerpts taken from a previous article written in 2020: "2020 Study of Advancements in Enterprise Risk and Governance.")

The Emergence of Enterprise-Wide Risk Management

In one critical study of corporate governance and enterprise-wide risk management, researchers from the Loyola University Chicago, School of Law (Ramirez & Simkins, 2008) lay out the barriers in effective board governance and specifically address systemic failings in current legal framework that fail to facilitate effective enterprise-wide risk management. "Historically, risk management within corporate American has not inspired confidence. Human resource management also poses risks to business."

The Loyola University Chicago, School of Law study (Ramirez & Simkins, 2008) singularly identified the two biggest gaps in enterprise-wide risk management, a.) less than robust risk analysis expertise in corporate American, and b.) the inability to management human risk factors.

The observations presented by Ramirez and Simkins remain relevant today and remain unaddressed in existing guidance today. Herbert Simon pointed out these weaknesses in his ground-breaking book, *"Administrative Behavior"*, followed by Dan Kahneman and Amos Tversky in "Prospect Theory".

Enterprise-wide risk management did not emerge until the 1990's and has continued to grow in importance albeit without widespread adoption. Enterprise risk management continues to be practiced in silos and fragmented across different organizations. COSO (committee of sponsoring organizations) is widely credited with defining ERM. COSO ERM is intentionally broad with a foundation built on internal controls over financial reporting and strategic risks. Other organizations, such as the Casualty Actuarial Society (CAS) offers a narrow definition of enterprise-wide risk management that encompass processes that lead to increases in stakeholder value creation. These two divergent views represent a lack of consensus on ERM as well as the fact that there is no *one-size-fits-all* approach that uniformly addresses risk profiles across industry type or operating models. Neither of these definitions of ERM has materially advanced risk practice.

The literature is clear on the aspirational goals of good ERM practice nevertheless there is little evidence that board governance has uniformly adopted pro-active risk best practice, particularly before adverse events arise. Examples abound of poor board governance prior to the 2002 Sarbanes-Oxley Act and after that serve as stark reminder that enterprise-wide risk management and strong board governance represent opportunities for enhanced performance. Successive failures in board governance begs the question, "what is the appropriate means of managing the risks inherent in a business environment on a comprehensive basis (Ramirez & Simkins, 2008)?

If enterprise-wide risk management (COSO ERM) is the best approach to managing risks, why aren't more firms using it? Evidence from studies and surveys indicates that, to date, only about 10% of major companies claim to have implemented many aspects of ERM, while almost all the others claim that they plan to do so in the future (Tonello, 2007) (Gates, 2006) (Schoening-Thiessen, 2005). To understand why ERM has not lived up to its promise we must examine the structural and cultural impediments to effective corporate governance and enterprise-wide risk management.

Structural impediments to advancements in corporate governance and enterprise-wide risk management

A Loyola University of Chicago Law study found that Sarbanes-Oxley (SOX) is fundamentally flawed and has failed to reform corporate governance and empower risk management (Ramirez & Simkins, 2008). The study goes further describing how state "corporate governance law and regulation largely fails to take modern financial [and risk-based] science on board." Boards are

given the autonomy to choose to operate with or without an ERM program or enterprise risk expertise.

SOX regulation was designed to address only the audit function and legal compliance, consequently failing to address risk management. SOX is a compliance mandate of internal controls over financial reporting disclosures and does not address or require a fulsome disclosure of all key risks that threaten the firm. Sarbanes-Oxley fails to contemplate behaviors that lead to fraud beyond internal control weakness such as withholding critical risk data from the board.

An exhaustive review of corporate financial statements finds wide disparity in the disclosure of risks and the processes for managing risks at the enterprise level. Boiler plate legal disclosures, common in financial statements, fail to fully inform stakeholders of a spectrum of risks facing the firm. In a recent public statement from SEC commissioner, Allison Herren Lee (January, 2020) stated, "investors are overwhelmingly telling us, through comment letters and petitions for rulemaking, that they need consistent, reliable, and comparable disclosures of the risks and opportunities related to sustainability measures, particularly climate risk."

"Investors have been clear that this information is material to their decision-making process, and a growing body of research confirms that. And MD&A is uniquely suited to disclosures related to climate risk; it provides a lens through which investors can assess the perspective of the stewards of their investment capital on this complex and critical issue."

"It is also clear that the broad, principles-based "materiality" standard has not produced sufficient disclosure to ensure that investors are getting the information they need—that is, disclosures that are consistent, reliable, and comparable. What's more, the agency's routine disclosure review process could be used to improve disclosure under the materiality standard, but in recent years there's been minimal comment on climate disclosure."

In organizations with no risk committees or CRO office the CEO becomes the risk manager by default because of the broad powers that accrue to the office of the executive. This is the natural result of broad public ownership combined with the CEO's power over board selections and the very minimal duties of board members under the law to supervise CEOs. Thus, under current corporate governance practices, the CEO is usually a risk silo (Ramirez & Simkins, 2008). Board governance has routinely failed to detect and prevent fraud formulated and executed by powerful CEOs as evidence of proof of the ineffectiveness of SOX regulation.

The conclusion of the study: Corporate governance is flawed by virtue of gaps in Sarbanes-Oxley, corporate law and regulatory financial disclosure that mandates compliance of accounting standards without equal weighting of risk management requirements and accountability at the board level. Sarbanes-Oxley provides internal audit and the board audit committee independence

but fails to make risk management independent inclusive of disclosure of material risks beyond weakness in internal controls over financial reporting. Information processing of key risks is cited as an opportunity to improve board governance in more than one study. Similar findings were noted in a second study by researchers examining the financial crisis of 2008 (Pirson & Turnbull, 2011).

In a (Pirson & Turnbull, 2011) study of the causes of the financial crisis of 2008 researchers noted that "hierarchical structures – as reflected in unitary boards – do not function well in dynamic and complex environments, partly because they are inflexible and do not support information processing as well as, for example, network structures". Network governance is "interfirm coordination that is characterized by organic or informal social system, in contrast to bureaucratic structures within firms and formal relationships between them. The study goes further to examine the root cause of inefficiencies in hierarchical structure through a focus on information processing at the board level defined as "systematic information processing problems."

The research in the (Pirson & Turnbull, 2011) study identified two reasons boards failed to manage risks in the 2008 mortgage financial crisis: (1) board members did not have access to relevant information of the risks incurred because they had no control over information supply and (2) board members were unable to process the available risk related information and lacked incentives or power to influence managerial decision making.

The paper found a systemic misfit between the information processing needs and the information processing capabilities in risk-related decision making at the board level during the crisis. Fligstein and Goldstein (2009) "observe that, in 2007, the US market for prime and sub-prime mortgages became highly concentrated with 25 firms being responsible for 90 per cent of the combined prime and sub-prime market. All 25 firms operated as centrally controlled hierarchies with a unitary board."

The study provided several examples where risk information within a firm was intentional withheld from the board by management. In one example, risk reports of violations exceeding the firm's risk appetite [mortgage securities] was withheld by the firm. In another example, disagreements between the CEO and the chairman of the board about risk taking was not shared with the board. The argument being that senior executives have great power to filter information from the boards about their activity and risk taking that could be instrumental to oversight. Boards do not have the power to compel risk information if they do not know it exists.

In a novel approach, the study (Pirson & Turnbull, 2011) noted behavioral science findings juxtaposing the supply of information with the ability of boards to absorb the complexity of the information presented to them. "Nevertheless, real-life time constraints would decrease the

transmission rates even further, as humans are limited in their ability to transmit and receive information of any type (Williamson, 1975; Williamson, 1979). Furthermore, there are few incentives for communicating risks in command and-control hierarchies."

The researchers conclude that there are structural problems in information processing between the board governance process and oversight of management. The information problems are described as: 1) Insufficient information access; 2) Insufficient information supply; 3) Information overload increases the risk of relevant information not being processed; and 4) Information bias and group dynamics distort rational information processing.

The remedies to these and other structural challenges to improving board governance and efficacious risk management practice is similar - independent risk committees and better risk information. Legal structures allow accumulation of power and decision-making at the executive level creating friction in risk information transmission between the board and senior executives. As noted earlier, boards are social constructs based on trust and information sharing. Boards operate efficiently during normal business conditions however during periods of financial crisis or significant uncertainty the social constructs on the board may become fragile and dysfunctional.

"Good" risk management is often cited by researchers, scholars and risk professionals as a process that improves decision-making. Risk management assists the organization achieve its goals and objectives by providing relevant information in a timely manner. When information flows are disrupted or disintermediated between the risk advisor(s) and decision-makers the process of good risk governance is circumvented.

A third study commissioned by COSO evaluated whether ERM as devised by the organization is an effective enterprise-wide risk framework. Institutional studies of enterprise risk are scarce and to date centered on qualitative methodology comprised of political, cultural, and technical activities (Lawrence & Suddaby, 2006; Perkmann & Spicer, 2008). "Drawing insights from the emerging literature on institutional work (e.g., Hwang & Colyvas, 2011; Lawrence & Suddaby, 2006; Lawrence, Suddaby, & Leca, 2011; Perkmann & Spicer, 2008; Suddaby & Viale, 2011)", evaluated innovations in management through enterprise risk practice. The Committee of Sponsoring Organizations (COSO) formulated a broadly adopted enterprise risk management framework in 2004.

This study, to the best of our knowledge, is the first to fully elaborate the notion of institutional work in accounting research (Hayne & Free 2014). The study suggests that COSO's ERM framework is an innovation in accounting, like cost accounting, the balanced score-card or risk-based auditing, a branch of management accounting. "In spite of these contributions, research on institutional work remains in its infancy; there are significant opportunities to describe and

explain the details of the ‘work’ involved. To this end, Hwang and Colyvas (2011, p. 62) conclude that institutional work is ‘‘... an umbrella concept and a rallying point’’ rather than a coherent framework.”

“COSO Board members themselves struggled to classify the organization in precise terms: COSO is kind of an odd organization, not just in terms of being a virtual organization but, you know, what is it? It’s not really a standard setter and yet it is kind of a standard setter. It’s not a company; it’s not a for-profit organization. And [so] I think, when COSO comes out with guidance, it carries a unique credibility because you can’t attribute their actions to a profit motive per se. (Douglas Prawitt, Interview 5).”

COSO filled a gap in formalizing accounting and audit work to detect, correct and mitigate internal control weakness across the enterprise. The granularity of audit work tended towards assessing internal controls, compliance, and risks at the operational level. A concentration on internal controls remediation should be recognized as a major contribution by COSO and is fundamental to a strong foundation on which to build a robust enterprise-wide risk framework.

On the other hand, after 35 years of focus on internal controls, where does the emerging field of risk professionals draw guidance and direction for the next generation of risk practice? What are the right tools to manage risks at the enterprise level? How does the risk function add value beyond compliance to standards? This study asked those questions in the 2020 Advancements in Enterprise Risk and Governance survey.

As the hybrid phase of Industry 4.0, the Fourth Industrial Revolution, emerges risk researchers and risk professional must begin to adopt more advanced methods risk practice that encompass a multidisciplinary approach to risks that should include virtual risks, human risk factors, scientific methods of risk analysis and cybersecurity. Thirty-five years is long enough to evaluate the evidence that COSO ERM, ISO 31000, NIST and other compliance and audit-based risk programs have not proven efficacious in practice. No additional evidence is needed however the human element in risk management is now the bottleneck in advancements in practice.

The baby boom generation of risk professionals have not been required to acquire the skills of modern risk professionals in the sciences, military, or any other discipline where risks have material impact. However, operational risks, human error and the technological complexity of cybersecurity demand a more rigorous approach to risk management training and application. The Covid-19 pandemic is but one example of the vulnerability in risk cognitive readiness to address asymmetric risks. Machine learning algorithms, Internet of Things connected devices and increased fragility in an Internet-based economy will expose the lack of preparedness that has been hidden by a lack of transparency in poor risk practice.