2008

Enterprise-Wide Risk Management and Corporate Governance.

Steven A. Ramirez
Loyola University Chicago, sramir3@luc.edu

Enterprise-Wide Risk Management and Corporate Governance

*Betty Simkins**

*Steven A. Ramirez***

I. INTRODUCTION: THE MANY FACES OF BUSINESS RISK

There has always been a fundamental tension between basic corporate governance precepts and the complexity of the business of the modern public corporation. Specifically, every corporation is to be managed by (or under the supervision of) the board of directors.[1] Directors are not generally required to have any particular expertise, other than being a "natural person."[2] Yet the modern corporation may well face a myriad of risks from disparate fields of business ranging from complex financial risk[3] to quality control regarding material manufactured in China.[4] If the board cannot understand and manage the full breadth of risks facing the modern public corporation, then such risks may not be disclosed to investors and impounded into decisions regarding the allocation of investment capital.[5]

---

* Betty Simkins, Ph.D., is the Williams Companies Professor of Business and Associate Professor of Finance at Oklahoma State University, Spears School of Business, Stillwater, Oklahoma.

** Steven A. Ramirez is Professor of Law and Director of the Business and Corporate Governance Law Center at Loyola University Chicago School of Law. The authors appreciate the helpful comments of John Fraser, Chief Risk Officer and Vice President, Internal Audit, at Hydro One.

1. *See* DEL. CODE ANN. tit. 8, § 141(a)(2007) (stating that every business "shall be managed by or under the direction of a board of directors").

2. *See id.* § 141(b) (noting that any additional qualification may be prescribed by the certificate of incorporation or bylaws).

3. Most recently, the subprime mortgage crisis seems to have had its roots in a systemic failure to identify and manage risks inherent in subprime lending. Because many such mortgages were securitized and distributed throughout the world financial system, large defaults caused large losses "roiling global credit markets." Glenn R. Simpson, *Lender Lobbying Blitz Abetted Mortgage Mess,* WALL ST. J., Dec. 31, 2007, at A1.

4. In 2007 Mattel saw its stock price plunge sixteen percent while it recalled millions of dangerous toys manufactured in China. Andrew Leckey, *Mattel Playing Better Overseas,* CHI. TRIB., Jan. 13, 2008, at C8.

5. It appears that a precipitating cause of the subprime mortgage crisis was non-disclosure of material risks to investors. Thus far, state and federal regulators have launched numerous

Recently, federal law imposed expertise requirements in connection with the management of the audit function for public companies. Under the Sarbanes-Oxley Act of 2002[6] (SOX), the "independent" auditor of a public corporation must report to an audit committee[7] which generally must include one "financial expert."[8] These requirements limit CEO control over the audit function and assure that there is some degree of appropriate financial expertise within the audit committee. Nevertheless, the audit function alone cannot comprehend all of the risks facing the modern public corporation.

This Article will explore the intersection of enterprise-wide risk management and corporate governance. The article concludes that enterprise-wide risk management can enhance the functioning of the corporation as well as the ability of capital markets to respond to risk, but that the current legal framework fails to facilitate this process. The Article suggests that disclosure requirements with respect to risk management would encourage superior transparency and management within the public corporation.

It seems axiomatic that today the public corporation too often fails to identify and manage the risks it faces. In late 2007, for example, a crisis in the subprime mortgage sector arose from one of the "worst miscalculations in the annals of risk management."[9] In fact, such systemic episodes of risk mismanagement can threaten macroeconomic performance and lead to financial crises.[10] Historically, risk

---

investigations relating to disclosure deficiencies in connection with the sale of subprime mortgages and securities backed by subprime mortgages. Karen Freifeld & David Scheer, *N.Y., Connecticut Probe Wall Street Loan Disclosures,* BLOOMBERG.COM, Jan. 12, 2008, http://www.bloomberg.com/apps/news?pid=20601087&sid=a8ry4S5dGsFs&refer=home. Naturally, the inability to comprehend risks results in a misallocation of capital, and the subprime mortgage crisis certainly is a "grotesque misallocation of capital." *See* Larry Elliott, *When Money Lenders Cry for Handouts,* THE GUARDIAN, Sept. 10, 2007, *available at* http://www.guardian.co.uk/business/2007/sep/10/businesscomment.ukeconomy (noting that "liberali[z]ing financial markets" has not in fact ended the misallocation of capital, as promised).

6. Sarbanes-Oxley Act of 2002, Pub. L. No. 107–204, 116 Stat. 745 (codified in scattered sections of 15 & 18 U.S.C.).

7. *Id.* § 204 (defining audit as an examination by an "independent public accounting firm").

8. *Id.* § 407.

9. Shawn Tully, *Wall Street's Money Machine Breaks Down,* FORTUNE, Nov. 12, 2007, *available at* http://money.cnn.com/magazines/fortune/fortune_archive/2007/11/26/101232838/index.htm.

10. *See* George Soros, *The Worst Market Crisis in 60 Years,* FIN. TIMES, Jan. 22, 2008, *available at* http://www.ft.com/cms/s/0/24f73610-c91e-11dc-9807-000077b07658.html (stating that risk mismanagement regarding subprime mortgages "spread to all collateralised debt obligations, endangered municipal and mortgage insurance and reinsurance companies and threatened to unravel the multi-trillion-dollar credit default swap market"). Soros also suggests that regulators failed to comprehend the risks posed by credit derivatives; this Article, however, is

management within corporate America has not always inspired confidence. Consider the following scenarios.

A. Bet-Your-Company Litigation

Pennzoil v. Texaco proved to be the ultimate exemplar of litigation risk.[11] On January 3, 1984, the Getty Oil Company board (along with affiliated entities) approved an oral agreement in principle to sell Getty to Pennzoil.[12] Texaco subsequently interfered with this agreement and a jury awarded $11 billion to Pennzoil against Texaco, the largest civil judgment ever.[13] Texaco ultimately declared bankruptcy and settled for $3 billion.[14] It seems unlikely that the Texaco board understood the risks of pursuing Getty.[15] The board also failed to understand the risks of the litigation itself.[16] An audit report would have been little help, as major litigation is not typically disclosed in audit reports, and is certainly not accompanied by an expert legal analysis that is meaningful to the board.[17]

---

limited to the corporate governance standards applicable to public companies and does not address financial institution regulation. *See id.*

11. Texaco, Inc. v. Pennzoil Co., 729 S.W.2d 768, 865 (Tex. App. 1987) (upholding a $7.53 billion actual damages verdict against Texaco).

12. *Id.* at 786; *see also* STEVE COLL, THE TAKING OF GETTY OIL 318–22 (1987) (describing the negotiations between Getty and Pennzoil and the belief that a deal had been made). During an emergency board meeting, the $112.50 per share oral agreement by Pennzoil was approved. *Id.* at 319–21. The exact repercussions and obligations of this "agreement in principle" became a point of contention for attorneys, businessmen, and advisors of Pennzoil and Getty Oil. *Id.* at 323–34.

13. Within forty-eight hours of the press release stating that the Getty board had approved an agreement in principle with Pennzoil, Texaco had made an offer, which was accepted by Getty, to pay $125 per share. *Id.* at 366–67, 371. Finding that Texaco knowingly interfered with the agreement between Pennzoil and Getty, a jury awarded Pennzoil $7.53 billion in compensatory damages and $3 billion in punitive damages. *Id.* at 470.

14. Robert H. Mnookin & Robert B. Wilson, *Rational Bargaining and Market Efficiency: Understanding* Pennzoil v. Texaco, 75 VA. L. REV. 295, 296 (1989). The $10.53 billion verdict began racking up interest at nearly $3 million per day. COLL, *supra* note 12, at 473. Texaco was almost immediately near bankruptcy until a federal judge, in what was later referred to as a "Fortune 500 exception to federalism," declared unconstitutional a Texas law requiring appellants to post a bond equal to the amount of the judgment against them. *Id.* Texaco was allowed to post $1 billion as bond versus the $12 billion bond that Texaco claimed would immediately force the company into bankruptcy. *Id.* The appellate court slightly reduced the judgment to $9.1 billion. *Id.* at 475.

15. Texaco's counsel told the firm that the worst case scenario for the Pennzoil claims was $250–500 million. COLL, *supra* note 12, at 408.

16. *Id.*

17. Under accounting standards, litigation risks deemed non-material need not be disclosed and material litigation risks are typically relegated to financial statement footnotes. *See* ACCOUNTING FOR CONTINGENCIES, Statement of Financial Accounting Standards No. 5, at 8, 11–13 (Fin. Accounting Standards Bd. 1975) [hereinafter FAS 5] (noting that the advice of legal counsel should be taken into consideration when determining whether the condition for a loss accrual is met).

B. Human Resources Mismanagement

Human resource mismanagement also poses risks to businesses. The most notorious example is Texaco Oil Company (and its unfortunate shareholders) during the time that racism within Texaco came to light. Texaco's human resources nightmare began in 1994, when African-American employees filed a class action lawsuit against the company, alleging pervasive racial discrimination.[18] The extent of Texaco's discriminatory misconduct was revealed in late 1996, when a senior executive released highly controversial tapes that apparently contained racial slurs emblematic of a racially hostile environment.[19] Once allegations of Texaco's misconduct surfaced, its shareholders suffered stunning losses, as its market capitalization plunged by $1 billion.[20] Subsequent reports demonstrated that the tapes were not isolated circumstances of racial bigotry, which instead pervaded Texaco's culture.[21] In 1997, Texaco paid $176 million, the largest amount paid in a racial discrimination suit at the time, to settle the class action claims of over 1300 African-American employees.[22] Texaco also suffered from a serious bout of negative publicity that caused investors to flee the company and consumers to threaten boycotts.[23] Certainly, it

18. Kurt Eichenwald, *Texaco Executives, On Tape, Discussed Impeding a Bias Suit*, N.Y. TIMES, Nov. 4, 1996, at A1.

19. *Id.* After being dismissed from Texaco and hiring personal counsel, Richard A. Lundwall, the senior coordinator for personal services in Texaco's finance department, delivered the tapes to the plaintiffs' attorney. *Id.* Lundell was responsible for keeping meeting minutes, and unknown to other executives, used a micro-cassette recorder to ensure their accuracy. *Id.* The tapes included a dialogue between the treasurer, Robert Ulrich, stating, "This diversity thing, you know how all the black jelly beans agree," and Lundwall responding, "That's funny. All the black jelly beans seem to be glued to the bottom of the bag." *Id.* Whether the tapes included the use of racial slurs is not known with certainty. *See* Steven A. Ramirez, *Diversity and the Boardroom*, 6 STAN. J. L. BUS. & FIN. 85, 108 n.125 (2000) (noting that Texaco used digital technology to conclude that no actual slur was used).

20. Kenneth Labich, *No More Crude at Texaco*, FORTUNE, Sept. 6, 1999, at 205. Texaco's share prices fell over 6% by the day after the release of the audio tapes. Stephen W. Pruitt & Leonard L. Nethercutt, *The Texaco Racial Discrimination Case and Shareholder Wealth*, 23 J. LAB. RES. 685, 688 (2002).

21. *See* BARI-ELLEN ROBERTS, ROBERTS V. TEXACO: A TRUE STORY OF RACE AND CORPORATE AMERICA 273 (1998) (detailing various disparaging remarks toward black workers at Texaco, such as being called "porch monkeys" and "orangutans" by supervisors).

22. Anne Reifenberg, *Texaco Settlement In Racial-Bias Case Endorsed by Judge*, WALL ST. J., Mar. 26, 1997, at B15. Following the settlement announcement, Texaco stock dropped 2.75%. Pruitt & Nethercutt, *supra* note 20, at 688. This was the largest racial discrimination settlement until 2000 when Coca-Cola settled a class action racial discrimination suit for $192.5 million. Greg Winter, *Coca-Cola Settles Racial Bias Case*, N.Y. TIMES, Nov. 17, 2000, at A1.

23. Peter Fritsch, *Trustee of Big Fund With Texaco Stock Says Tape Shows 'Culture of Disrespect,'* WALL ST. J., Nov. 6, 1996, at A5 (stating that the fund was considering selling because of discrimination and its impact on performance); Allanna Sullivan & Peter Fritsch,

appears that the board failed to control the risk of allowing racial hostility.

C. Internal Non-Controls

In a landmark case of risk mismanagement, Barings Bank was brought down by the losses incurred by a single rogue trader.[24] Barings Bank's flawed risk management of its trading activities in Singapore between 1993 and 1995 enabled one of its traders, Nick Leeson, to incur huge losses free of effective supervision.[25] Leeson acted both as trader and as manager with regard to his activities.[26] Thus, Leeson was essentially supervising himself.[27]

Due to the absence of oversight, Leeson was able to report losses as gains to Barings in London.[28] Specifically, Leeson altered the branch's error account, known by its account number 88888 as the "five-eights account," to prevent London from receiving reports of losses.[29] By 1994, Leeson began to aggressively trade in futures and options on the Nikkei index.[30] After two years of large losses, the bank's auditors found accounting discrepancies that led to the discovery of Leeson's trading.[31] Nick Leeson's activities generated losses in excess of $1.3 billion.[32] Barings collapsed on February 26, 1995.[33]

Recently, a single rogue trader imposed a $7.2 billion dollar loss on a large French bank, suggesting that risk management in this area has hardly improved.[34] Leeson himself suggests that the core problem is

---

Texaco Chairman Meets Advocates for Civil Rights, WALL ST. J., Nov. 13, 1996, at B3 (discussing planned boycotts and picketing of Texaco stations).

24. Editorial, *Rogue Traders*, FIN. TIMES, Jan. 25, 2008, at 14.

25. Laura Proctor, Note, *The Barings Collapse: A Regulatory Failure, or a Failure of Supervision?*, 22 BROOK. J. INT'L L. 735, 736–37, 751–59, 764–65 (1997) (examining the problems of supervision and lack of internal controls that caused the collapse).

26. *Id.* at 753.

27. *See* Proctor, *supra* note 25, at 753–54 (stating that Baring's selection of the "cheapest and least complicated" methods meant Leeson had unfettered control to make the trades he wanted).

28. *Id.* at 739.

29. *Id.* at 739–40.

30. *Id.* at 738.

31. Richard W. Stevenson, *Singapore Study Cites Barings Executives*, N.Y. TIMES, Oct. 18, 1995, at D6.

32. *Rogue Trader Says Banks Lack Risk Mgmt*, BOSTON GLOBE, Jan. 24, 2008, *available at* http://www.boston.com/news/world/europe/articles/2008/01/24/rogue_trader_says_banks_lack_risk_mgmt [hereinafter *Rogue Trader*]. Founded in 1762 and still run by the Barings family, Barings Bank had the distinguished title of England's oldest bank and had financed hefty projects such as the Napoleonic wars. Tim Rayment, *History Repeats Itself at Barings*, SUNDAY TIMES, Feb. 26, 1995, at 1–2 (chronicling Barings Bank's notable history and spectacular decline).

33. Procter, *supra* note 25, at 735.

34. *Rogue Trader*, *supra* note 32.

that too often the focus is on "profit, profit now" rather than proper risk management.[35]

D. Accounting Fraud and Weak Corporate Governance

The importance of corporate governance and the risk of accounting fraud was manifest with the unexpected 2001 collapse of Enron.[36] Enron focused excessively on its stock price. The strategy of the Chief Executive Officer Kenneth Lay and President Jeffrey Skilling was to continually enter new markets and businesses to create hype about the firm and its stock.[37] Enron used off-balance sheet entities to conceal losses and prop up earnings.[38] Enron's CFO ultimately made tens of millions of dollars in just a few years from managing some of these "special purpose entities."[39] The accounting fraud committed at Enron led to the collapse of Arthur Andersen, the accounting firm that audited Enron's books and approved the accounting treatment of the partnerships.[40]

Enron's collapse was followed by a series of other massive corporate scandals in 2002 including Bristol-Myers Squibb, Qwest, Xerox, WorldCom, and Global Crossing, among others.[41] These scandals highlighted serious shortcomings in corporate governance.[42] Congress soon passed the Sarbanes-Oxley Act of 2002 in an effort to reform the audit function at public firms in particular and to reform corporate governance in general.[43]

---

35. *Id.*

36. Peter Elkind & Bethany McLean, *Enron on Trial: Judgment Day*, FORTUNE, Jan. 23, 2006, at 58, *available at* http://money.cnn.com/2006/01/12/news/companies/enron1_fortune/index.htm.

37. Paul M. Healy & Krishna G. Palepu, *The Fall of Enron*, 17 J. ECON. PERSP. 3, 4 (2003).

38. *See* WILLIAM C. POWERS, JR. ET. AL., Report of Investigation, 4, 171 (Feb. 1, 2002) (finding that some of the most significant transactions were "designed to accomplish favorable financial statement results, not to achieve *bona fide* economic objectives or to transfer risk," and were structured to keep debt off the balance sheets).

39. *Id.* at 3–4.

40. Joseph Radigan, *Closing the Books on Anderson*, CFO.COM, Aug. 30, 2002, http://www.cfo.com/article.cfm/3006242?f=related.

41. Steven A. Ramirez, *Fear and Social Capitalism*, 42 WASHBURN L.J. 31, 31–32 (2002).

42. *See id.* at 61–62 (listing some shortcomings in corporate governance, including corporate management using its power to influence legislatures to lessen corporate regulation, managers being able to disregard their duty of care, and managers being able to receive millions in compensation while their shareholders lose money).

43. *See supra* notes 6–8 and accompanying text (requiring audits to be done by an independent public accounting firm).

Each of these scenarios raises the same question: what is the appropriate means of managing the risks inherent in the business environment on a comprehensive basis?

Part II provides an overview of the emerging science of Enterprise-Wide Risk Management in order to determine the most successful approach to managing the risks facing the business enterprise. Part III reviews current corporate governance mandates in an effort to determine the efficacy of risk management mechanisms currently in place. Part IV explores the gap between current legal and regulatory requirements regarding risk management and evidence of best practices of risk management with a view towards assessing whether any legal or regulatory adjustments are needed. This Article concludes that clarifying action by the SEC is advisable to shift the arena for the resolution of this question from the courtroom to the marketplace. In other words, as long as shareholders have access to information regarding corporate risk management, regulators should allow the market to sort the value of risk management regimes, at least for now.

II. THE EMERGENCE OF ENTERPRISE-WIDE RISK MANAGEMENT

To examine the emergence of enterprise-wide risk management ("ERM"), it is important to first discuss the concept of risk and to provide a brief history of risk management. The word "risk" in English derives from the Italian word *risicare*, which means "to dare."[44] The Chinese symbol for risk, which dates back to ancient times, consists of two symbols: the first represents "danger" and the second "opportunity." These two symbols imply that risk is a strategic combination of vulnerability (i.e., danger) and opportunity.[45]

Managing risk, or what is commonly referred to as "risk management," is a concept that dates back thousands of years to when early visionaries tried to understand risk, manage aspects of risk that were manageable, and weigh the consequences of what they could not manage.[46] For example, there is early evidence suggesting that risk

44. PETER L. BERNSTEIN, AGAINST THE GODS: THE REMARKABLE STORY OF RISK 8 (1996).

45. Tom Aabo et al., *The Rise and Evolution of the Chief Risk Officer: Enterprise Risk Management at Hydro One*, J. APPLIED CORP. FIN., Summer 2005, at 62, 62.

46. For an excellent discussion on the history of risk, see generally BERNSTEIN, *supra* note 44, which traces the development of risk from the time of the ancient Greeks through the modern era. Early examples of risk management can be found in the Bible. *See* Don M. Chance, *A Chronology of Derivatives*, 2 DERIVATIVES Q. 53 (1995). Chance states:

> 1700 B.C. Genesis, Chapter 29. Jacob buys an option costing seven years' labor to marry Laban's daughter Rachel. Laban reneges and forces Jacob to marry older daughter Leah. Jacob buys another option to work seven more years to marry Rachel; ends up with two wives, twelve sons (patriarchs of the twelve tribes of Israel), and

management using commodity futures trading took place in India around 2000 B.C.[47] The basic principle of a central market to manage risk dates back to ancient Greek and Roman markets.[48] Beginning in the 1100s, sellers at medieval trade fairs signed contracts, called *letters de faire*, promising future delivery of the items they sold.[49] At the height of the Roman Empire, trading centers, called *fora vendalia*, were used to trade commodities the Romans obtained from throughout their empire.[50] Historical records indicate that futures contracts were first used in Japan in the 1600s.[51] The feudal lords of Japan used a market called *cho-ai-mai* (rice trade on book) to manage the volatility in rice prices caused by bad weather and warfare.[52] During the 1600s, formal futures markets emerged in Europe.[53]

The history of modern risk management using futures trading began in the midwestern United States in the early 1800s in the area of grain trade.[54] This history of managing the price risk of agricultural commodities is tied closely to the development of commerce in Chicago, a city strategically located at the base of the Great Lakes and close to the farmlands of the midwest. Problems of supply and demand,

---

considerable domestic tension. Some disagreement exists, however, over whether Jacob held an option or a forward contract, the latter obligating him to the marriage.

> Genesis, Chapter 41. According to Joseph's advice, an Egyptian pharaoh, anticipating seven years of feast followed by seven years of famine, executes hedge by storing corn. Joseph is put in charge of administering the program.

Id. at 53–54.

47. *See* DARRELL DUFFIE, FUTURES MARKETS (1989) (presenting a very broad perspective on futures markets).

48. *See* RICHARD J. TEWELES & FRANK J. JONES, THE FUTURES GAME 6 (2d ed. McGraw-Hill 1987) (1974) (noting that the Greek and Roman markets used modern trade practices, such as contracts for future delivery).

49. BERNSTEIN, *supra* note 44, at 306.

50. CHICAGO BOARD OF TRADE, COMMODITY TRADING MANUAL (Patrick J. Cantania et al. eds., 1994).

51. BERNSTEIN, *supra* note 44, at 306.

52. *Id. See also* TEWELES & JONES, *supra* note 48, at 8 (discussing the "rice ticket" practice used to combat income instability).

53. These medieval trade fairs are important to the eventual development of organized markets to manage risk because they helped establish the principles of self-regulation, arbitration, and formalized trading practices. For example, in medieval England, a code called the Law Merchant established standards of conduct acceptable to local authorities for the use of contracts, bills of sale, letters of credit, and transfers of deeds, among other items. These early formalized methods of trading practices established principles for self-regulation in England's Common Law, which were later adopted by U.S. commodity exchanges.

54. TEWELES & JONES, *supra* note 48, at 9 (noting that the history of modern futures trading began on the Midwestern frontier in the early 1800s. It was tied closely to the development of commerce in Chicago and the grain trade in the Midwest).

transportation, and storage led logically to the development of futures markets in Chicago.[55]

In the 1950s, breakthroughs and advancements in the mathematics for quantifying financial risks were developed, beginning with Harry Markowitz's mean-variance theory of portfolio selection.[56] Markowitz's theory provided a framework for portfolio selection and quantifying the risk-return trade-off.[57] Building on Markowitz's work, William Sharpe and John Lintner developed the capital asset pricing model ("CAPM"), which became the seminal model for measuring the risk of a security.[58] In 1973, Fisher Black and Myron Scholes published their pathbreaking paper for option pricing, which quickly became the most important development in finance that influenced practice. In 1997, Scholes, together with Robert Merton, was a co-recipient of the Nobel Prize in Economics.[59] Collectively, these studies provided a method to quantify risk that revolutionized the field of finance and economics.[60] It was now possible to quantify risk as never before.[61]

---

55. Other agricultural commodity trading soon followed. TEWELES & JONES, *supra* note 48, at 1–10. The New York Cotton Exchange was established in 1870 and shortly afterward governed cotton futures trading. *Id.* Futures trading on the New Orleans Cotton Exchange began around 1870 and other successful futures exchanges emerged around the same time (i.e., New York Produce Exchange, the Milwaukee Chamber of Commerce, the Merchant's Exchange of St. Louis, the Duluth Board of Trade, and the Kansas City Board of Trade). *Id.*; GEORGE W. HOFFMAN, FUTURES TRADING UPON ORGANIZED COMMODITY MARKETS IN THE UNITED STATES (1932) (further addressing the development of commodity exchanges). The basic principles of futures trading were now in place, creating the catalyst for this infant industry to revolutionize commodity trading and risk management around the world. *See* THOMAS A. HIERONYMUS, ECONOMICS OF FUTURES TRADING FOR COMMERCIAL AND PERSONAL PROFIT (Commodity Research Bureau, Inc. 1977) (1971) (providing a basic study of futures trading).

56. *See* Harry Markowitz, *Portfolio Selection*, 7 J. FIN. 77 (1952) (introducing the variance of return theory); HARRY M. MARKOWITZ, PORTFOLIO SELECTION: EFFICIENT DIVERSIFICATION OF INVESTMENT (1959) (presenting techniques for the analysis of portfolios of securities).

57. *See* Robert C. Merton, *Influence of Mathematical Models in Finance on Practice: Past, Present, and Future*, *in* MATHEMATICAL MODELS IN FINANCE 1, 3 (1995) (providing a more comprehensive discussion on mathematical breakthroughs in finance).

58. William F. Sharpe, *Capital Asset Prices: A Theory of Market Equilibrium Under Conditions of Risk*, 19 J. FIN. 425 (1964); John Litner, *The Valuation of Risky Assets and the Selection of Risk Investments in Stock Portfolios and Capital Budgets*, 47 REV. ECON. & STAT. 13 (1965).

59. *See* Nobelprize.org, http://nobelprize.org/nobel_prizes/economics/laureates/1997/index.html (announcing Robert C. Merton and Myron S. Scholes as co-recipients of the 1997 Nobel Prize in Economic Sciences "for a new method to determine the value of derivatives").

60. Press Release, Nobelprize.org, The Sveriges Riksbank Prize in Economic Sciences in Memory of Alfred Nobel 1997 (Oct. 14, 1997), *available at* http://nobelprize.org/nobel_prizes/economics/laureates/1997/press.html.

61. It is important to note that in the 1730s, Abraham de Moivre published the first derivation of the normal (or Gaussian) distribution, also known as the bell curve, and established the concept

Prior to the 1970s, interest rates and foreign exchange rates were fairly stable and inflation was not yet a concern.[62] All of this changed in 1971 with the collapse of the Bretton Woods system, which had essentially fixed the relative value of major exchange rates to the U.S. dollar.[63] Exchange rate volatility increased dramatically due to a move to floating exchange rates.[64] Furthermore, relatively high inflation from the late 1960s to the early 1980s created substantial interest rate risk.[65] During the 1970s, oil price risk became a major factor when the Organization of Petroleum Exporting Countries ("OPEC") restricted production to increase prices.[66] Financial risks quickly emerged as a top concern in risk management. Demand increased rapidly for tools to manage risk, and mathematics provided them.[67] The world witnessed rapid innovation and evolution in the understanding and management of financial risks. Within a few years, institutions and entire industries that utilized these tools emerged and the word "derivatives" became a commonplace term.[68]

Enterprise-wide risk management, or ERM, first emerged as a recognized new approach to risk management in the 1990s. ERM, in our opinion, is a natural evolution of the process of risk management, and represents a more advanced and sophisticated approach to

---

of standard deviation. His work is essential to modern techniques for quantifying risk. *See* ABRAHAM DE MOIVRE, THE DOCTRINE OF CHANCES (3rd ed. 1738).

62. *See* HAROLD JAMES, INTERNATIONAL MONETARY COOPERATION SINCE BRETTON WOODS 148 (1996) (study on postwar economic monetary cooperation).

63. *Id.* at 205.

64. *Id.* at 220.

65. *See id.* at 343 fig.11–3 (charting interest rates).

66. *Id.* at 253–54.

67. For a discussion of the evolution of risk management instruments for managing exchange rate, interest rate, and commodity-price risk, see chapter 1 of CHARLES W. SMITHSON, CLIFFORD W. SMITH, JR., & K. SYKES WILFORD, MANAGING FINANCIAL RISK 18–22 (1998).

68. In academics, risk management as an organized field of study was first developed in the 1950s by insurance professors. The first risk management text, *Risk Management and the Business Enterprise*, co-authored by Robert Mehr and Bob Hedges, was published in 1963. *See also* Stephen P. D'Arcy, *Enterprise Risk Management*, 12 J. RISK MGMT. OF KOREA 207 (2001) (discussing the history of enterprise risk management). The primary focus of risk management at that time in education was on what is now called hazard risk and the focus was on "pure risks." Pure risks can be defined as having two outcomes: a loss or no loss. In other words, the focus was purely on managing downside risk. This area developed its own terminology and techniques for analyzing risk. The academic study of financial risk management began in the 1980s with the publication of the first text in this area by Cox and Rubinstein in 1985. *See* JOHN C. COX & MARK RUBINSTEIN, OPTION MARKETS (1985). This area also developed its own terminology and techniques for analyzing risk. *Id.*

managing risk.[69] Some sources have referred to ERM as a new risk management paradigm.[70]

Currently, many organizations still continue to address risk in "silos," with the management of insurance, foreign exchange risk, operational risk, credit risk, and commodity risks each conducted as narrowly-focused and fragmented activities. Under ERM, all risk areas function as parts of an integrated, strategic, and enterprise-wide system. While risk management is coordinated with senior-level oversight, employees at all levels of the organization using ERM are encouraged to view risk management as an integral and ongoing part of their jobs. Figure 1 illustrates the differences between these two approaches.

FIGURE 1: Old and New Paradigms of Risk Management

Old Paradigm	New Paradigm
Fragmented Departments manage risks independently (silos)	**Integrated and Enterprise-Wide** Coordinated with senior-level oversight, risk management culture
Ad hoc Risk management done when thought appropriate	**Continuous** Ongoing process
Narrowly focused Addresses primarily insurable risk and financial risks	**Broadly focused** Addresses all business risks and opportunities

The Committee of Sponsoring Organizations of the Treadway Commission ("COSO") defines enterprise-wide risk management as:

> [A] process, [a]ffected 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

69. Other terms have been used interchangeably to also refer to the concept of enterprise risk management, including: integrated, strategic, firmwide, and enterprise-wide. COX & RUBINSTEIN, *supra* note 68.

70. *See* THOMAS L. BARTON, WILLIAM G. SHENKIR, & PAUL L. WALKER, MAKING ENTERPRISE RISK MANAGEMENT PAY OFF (2002); Mark S. Beasley, Richard Clune, & Dana R. Hermanson, *Enterprise Risk Management: An Empirical Analysis of Factors Associated with the Extent of Implementation*, 24 J. OF ACCT. & PUB. POL'Y 521 (2005).

> entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.[71]

The COSO definition is intentionally broad and deals with risks and opportunities affecting value creation or preservation. However, other groups define enterprise-wide risk management more narrowly. For example, the Casualty Actuarial Society ("CAS") defines enterprise-wide risk management as, "the process by which organizations in all industries assess, control, exploit, finance, and monitor risks from all sources for the purpose of increasing the organization's short and long term value to its stakeholders."[72] The CAS enumerates the types of risk subject to enterprise risk management as hazard, financial, operational, and strategic.[73] The important "take away" is that there is no "one-size-fits-all" consensus on how to view enterprise-wide risk management across all organizations or companies globally.

While there are theoretical and practical arguments for the use of ERM,[74] the main external drivers for its implementation have been studies such as the Joint Australian/New Zealand Standard for Risk Management,[75] COSO,[76] the Group of Thirty Report in the United States (following derivatives disasters in the early 1990s),[77] the Criteria of Control model developed by the Canadian Institute of Chartered Accountants ("CoCo"),[78] the Toronto Stock Exchange Dey Report in

71. *See* COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION, ENTERPRISE RISK MANAGEMENT—INTEGRATED FRAMEWORK 2 (2004), *available at* http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf [hereinafter COSO, ENTERPRISE RISK MANAGEMENT].

72. *See* CASUALTY ACTUARIAL SOCIETY, ENTERPRISE RISK MANAGEMENT COMMITTEE, OVERVIEW OF ENTERPRISE RISK MANAGEMENT 8 (2003), *available at* http://www.casact.org/research/erm/overview.pdf.

73. *Id.* at 8–10.

74. This discussion draws extensively from Professor Simkins' publication. *See* Aabo, et. al., *supra* note 45.

75. JOINT AUSTRALIAN/NEW ZEALAND STANDARD, RISK MANAGEMENT (2004) (providing the first articulation of practical enterprise risk management). This guide, first published in 1995, covers the establishment and implementation of the risk management process involving the identification, analysis, evaluation, treatment, and ongoing monitoring of risks.

76. COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION, INTERNAL CONTROL—INTEGRATED FRAMEWORK (Sept. 1992).

77. GROUP OF THIRTY, DERIVATIVES: PRACTICES AND PRINCIPLES (July 1993).

78. CRITERIA OF CONTROL BOARD, & CANADIAN INSTITUTE OF CHARTERED ACCOUNTANTS, GUIDANCE ON CONTROL (1995).

Canada following major bankruptcies,[79] and the Cadbury Report in the United Kingdom.[80]

Additionally, major legal developments such as the New York Stock Exchange Listing Standards and the interpretation of recent Delaware case law on fiduciary duties, among others, have provided an additional force for ERM.[81] Large pension funds have become more vocal about the need for improved corporate governance, including risk management, and have stated their willingness to pay premiums for the stock of firms with strong, independent board governance.[82]

ERM is now developing into a tool that can be used to enhance firm value.[83] For example, security rating agencies such as Moody's Investors Service and Standard & Poor's ("S&P") include whether a company has an ERM system as a factor in their ratings methodology for financial institutions and insurance companies. On November 15, 2007, S&P released a request for comment on their guidelines for rating non-financial companies, specifically regarding ERM.[84] In 2004, Moody's announced that it will perform formal risk management assessments as part of the ratings process.[85] The Moody's assessment framework addresses four key risk areas: Risk Governance, Risk Management, Risk Analysis and Quantification, and Risk Infrastructure

79. COMMITTEE ON CORPORATE GOVERNANCE IN CANADA, TORONTO STOCK EXCHANGE, WHERE WERE THE DIRECTORS? GUIDELINES FOR IMPROVED CORPORATE GOVERNANCE IN CANADA (1994).

80. COMMITTEE ON THE FINANCIAL ASPECTS OF CORPORATE GOVERNANCE, CODE OF BEST PRACTICE 16–19 (Dec. 2002), *available at* www.ecgi.org/codes/documents/cadbury.pdf.

81. *See* Mark Beasley, Don Pagach, & Richard Warr, *Information Conveyed in Hiring Announcements of Senior Executives Overseeing Enterprise-Wide Risk Management Processes* (forthcoming), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=916783.

82. *See generally* JAY A. CONGER, EDWARD E. LAWLER, III & DAVID FINEGOLD, CORPORATE BOARDS: NEW STRATEGIES FOR ADDING VALUE AT THE TOP (2001).

83. Risk management in general has been shown to increase firm value. *See* Charles W. Smithson & Betty J. Simkins, *Does Risk Management Add Value? A Survey of the Evidence*, 17 J. OF APPLIED CORP. FIN. 8, 8 (2005) ("Although the research . . . is not uniformly supportive of the corporate use of derivatives, the bulk of it reinforces the idea that corporate risk management is a value-adding activity.").

84. Standard & Poor's Ratings Direct, Request for Comment: Enterprise Risk Management Analysis For Credit Ratings of Nonfinancial Companies (Nov. 15, 2007), http://www.standardandpoors.com/ratingsdirect. For additional discussion on enterprise risk management and its affect on credit ratings, see Prodyot Samanta, Richard Barnes & Mark Puccia, Standard & Poor's Rating Direct, Accessing Enterprise Risk Management Practices of Financial Institutions (Sept. 22, 2006), http://www2.standardandpoors.com/spf/pdf/products/ICR_Article_CriteriaAssessingEnterpriseRisk.pdf and *Morgan Stanley Roundtable on Enterprise Risk Management and Corporate Strategy*, 17 J. OF APPLIED CORP. FIN. 32 (2005).

85. *See* HERVE GENY & JAMES HYDE, MOODY'S INVESTOR SERVICES, RISK MANAGEMENT ASSESSMENTS (2004), http://www.moodys.com/moodys/cust/research/MDCdocs/02/2002900000432768.pdf?search=5&searchQuery=Risk+Management+Assessments&click=1.

and Intelligence. The following statement by Moody's summarizes its view:

> Increasing numbers of companies are undertaking enterprise-level approaches to risk—a more encompassing and systematic review of potential risks and their mitigation than most companies have undertaken in the past. Business units are tasked with identifying risks and, where possible, quantifying and determining how to mitigate them. These assessments typically are rolled up to a corporate level, sometimes with direct input from the board or audit committee. These assessments have often been relatively broad, focusing on reputation, litigation, product development, and health and safety risks, rather than focusing solely on financial risks. Where we have seen these assessments implemented, we have commented favorably, particularly when the board or the audit committee is actively involved. [86]

ERM continues to increase in importance, partly as the result of the Sarbanes-Oxley Act of 2002, which places greater responsibility on the board of directors to understand and monitor an organization's risks, particularly in the context of audit issues.[87]

In response to this need for guidance in the implementation of ERM, a number of frameworks have been developed. Perhaps the most widely known framework is the COSO's *Enterprise Risk Management—Integrated Framework*, released in 2004.[88] This framework provides a benchmarking tool to help organizations develop a road map toward full ERM implementation.[89] Under ERM, risks can be viewed as falling into two broad areas: core risks (risks which a firm should have a competitive advantage to handle in their business model) and non-core risks (risks which could be hedged by the business or transferred through risk management techniques).[90]

Given the overwhelming incentives and pressures to employ an enterprise-wide approach to risk management, an obvious question to ask is: "Why are more firms not using ERM?" 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

86. Moody's Investors Service, *Moody's Findings on Corporate Governance in the United States and Canada: August 2003–September 2004* (Oct. 5, 2004), *available at* www.moodys.com (search "Document Title" for "Moody's Findings on Corporate Governance"). *See also* Samanta, Barnes & Puccia, *supra* note 84; Beasley, Pagach & Warr, *supra* note 81.

87. *See supra* notes 6–8 and accompanying text (discussing responsibilities of the board of directors under Sarbanes-Oxley).

88. *See* COSO, ENTERPRISE RISK MANAGEMENT, *supra* note 71.

89. *Id.*

90. *Id.*

others claim that they plan to do so in the future.[91] One deterrent is the need for more information on implementing ERM, including case studies and educational materials.[92] A study by the Association of Financial Professionals notes that most senior financial professionals find their activities evolving into a more strategic role, which they believe requires more education and training to meet future challenges.[93] Also, common misconceptions about enterprise-wide risk management impede many firms' progress in this area.[94] Beasley, Clune, and Hermanson find that firms with ERM programs (or those that are further along in ERM implementation) are more likely to have a chief risk officer; greater independence on the board of directors; the support of the CEO and CFO; the presence of a Big Four auditor; a larger size; an operation in banking, education, or insurance; and either have more international focus or are an international company.[95]

Boards of directors are now taking risk more seriously. A 2005 survey by Lloyds and the Economist Intelligence Unit finds that 40% of boards spend more than 10% of their time on formal risk management, which is a dramatic increase from the ten percent response rate received on a similar study conducted three years earlier.[96] The survey reveals that this increase in board awareness is largely due to governance and

91. *See* MATTEO TONELLO, THE CONFERENCE BOARD, MERGING GOVERNANCE PRACTICES IN ENTERPRISE RISK MANAGEMENT (2007) (describing the elements of a comprehensive ERM program, discussing the legal foundation for ERM, and explaining how disclosure to stakeholders can be enhanced by ERM); Stephen Gates, *Incorporating Strategic Risk into Enterprise Risk Management: A Survey of Current Corporate Practice*, 18 J. OF APPLIED CORP. FIN. 81, 83 (2006) (stating that 11% of companies claim to have "fully implemented" ERM programs, 22% stated they were "actively in the process," and 23% stated they were "in the planning and preparation phase"); KAREN SCHOENING-THIESSEN, THE CONFERENCE BOARD OF CANADA, ENTERPRISE RISK MANAGEMENT: INSIDE AND OUT (2005) (providing information on what organizations are doing at each of the three stages of ERM—strategy development, strategy implementation, and maintenance).

92. For a few examples of case studies describing the implementation of enterprise risk management, see Aabo, et. al., *supra* note 45, at 62; Scott E. Harrington, Greg Niehaus & Kenneth J. Risko, *Enterprise Risk Management: The Case of United Grain Growers*, 14 J. OF APPLIED CORP. FIN. 71 (2002) (describing how United Grain Growers combined protection against financial risk and conventional insurance risk using an integrated risk management policy provided by Swiss Re); *see also* Barton, et. al., *supra* note 70 (listing additional case studies on enterprise risk management).

93. ASSOCIATION FOR FINANCIAL PROFESSIONALS, THE EVOLVING ROLE OF TREASURY: REPORT OF SURVEY RESULTS 3, 5–6 (2003), *available at* www.afponline.org/pub/pdf/AFPTreasury_%20survey.pdf.

94. John R. S. Fraser & Betty J. Simkins, *Ten Common Misconceptions About Enterprise Risk Management*, 19 J. APPLIED CORP. FIN. 75 (2007).

95. Beasley, et al., *supra* note 70, at 521–22.

96. LLOYD'S & THE ECONOMIST INTELLIGENCE UNIT, TAKING RISK ON BOARD: HOW GLOBAL BUSINESS LEADERS VIEW RISK 1, 5 (2005).

regulatory factors.[97] While the boards are more aware of risk, this does not mean they have necessarily implemented a process to identify or mitigate risk. The study reveals that about 20% of the companies surveyed suffered significant loss from a failure to manage risk within the previous year and that 56% had experienced at least one "near miss."[98]

Overall, these studies point out that chief executives and boards of directors need to have a thorough understanding of the key risks in the organization and what is being done to manage them. Directors need to make sure they ask the right questions and that the right checks and balances are in place. Directors need to understand that, if properly implemented, ERM provides a significant opportunity for competitive advantage and can enhance shareholder value. While the literature and evidence to date makes it clear that there is no single ERM implementation process that works for every board and every company, this is no excuse for inaction. History has proven that losses from risk can strike ill-prepared companies with hurricane force. ERM programs can help organizations succeed and prosper, if they are properly implemented and monitored by chief officers and the board of directors. Delegates to the Conference Board Governance Center's Corporate/Investor Summit held in London in July 2005 stated:

> [W]idespread adoption of an enterprise risk management (ERM) framework should be encouraged as an effective process to assess and respond to strategic and operating risks, is crucial not only to bring clarity to the long-term strategic direction a business should take, but also to clearly communicate such long-term strategy to the market.[99]

III. CORPORATE GOVERNANCE LAW AND RISK MANAGEMENT

As demonstrated above, ERM has evolved in a manner that supports enhanced financial management through enhanced identification and management of all the risks facing the corporation.[100] This systematic and comprehensive approach to risk management has been empirically tested and the results show that ERM delivers upon its theoretical promises.[101] The key elements of successful ERM programs, insofar as

97. *Id.*

98. *Id.* at 6.

99. MATTEO TONELLO, THE CONFERENCE BOARD, REVISITING STOCK MARKET SHORT-TERMISM 43 (2006). Also, for a good reference on directors and risk management, see HUGH LINDSAY, THE CONFERENCE BOARD, 20 QUESTIONS DIRECTORS SHOULD ASK ABOUT RISK (2d ed. 2006).

100. *See supra* Part II (describing the emergence of enterprise-wide risk management).

101. *See supra* notes 83–87 and accompanying text (detailing the benefits to firms that use ERM).

corporate governance is concerned, are comprehensive and transcendent risk management that operates to avoid silos, and senior level (preferably board level) involvement in risk management.[102] Unfortunately, corporate governance law and regulation largely fails to take modern financial science on board.

Instead, corporate governance law at the state level gives corporate management autonomy to implement ERM or to have no enterprise-wide risk management frameworks in place at all. Boards are simply given the power to manage the corporation as they see fit and do not have any risk management expertise or controls in place.[103] In the public corporation, this means that the CEO is the institutional center of risk management.[104] 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.[105] Thus, under current corporate governance practices, the CEO is usually a risk silo.

A CEO-centric model of risk management need not lead to suboptimal results. Ideally, the CEO's interests will align with the shareholders in a manner that encourages appropriate risk management.[106] Nevertheless, the CEO could just as easily be tempted

---

102. *See supra* note 94 and accompanying text (noting that misconceptions about ERM have impeded firms' progress in this area); *infra* notes 103–108 and accompanying text (discussing the result of a CEO-centric model of risk management).

103. *See, e.g.*, *supra* notes 1–2 and accompanying text (noting the complete absence of qualifications required to be on a board of directors under Delaware law).

104. There is no legal requirement that all operational authority be centralized in the CEO. From a business perspective, it seems that a single strategic vision can best be pursued by a single individual authority. *See* ALAN GREENSPAN, THE AGE OF TURBULENCE: ADVENTURES IN A NEW WORLD 429 (2007) ("CEO control and the authoritarianism it breeds are probably the only way to run an enterprise successfully.").

105. *See* Steven A. Ramirez, *The Special Interest Race to CEO Primacy and the End of Corporate Governance Law*, 32 DEL. J. CORP. L. 345, 358–67 (2007) (comprehensively summarizing legal indulgences extended to management and concluding that "considering the legal trajectory of corporate governance law for publicly held companies, it is not surprising that investment experts like John Bogle see a 'pathological mutation' . . . that exalts the interests of the CEO over all others").

106. This hope was the reason why many companies used stock related compensation:

> Since the mid-1990s, American CEOs have been paid primarily in megagrants of stock and stock options—especially high-octane options—on the theory that having lots of "skin" in the game better aligns CEO interests with those of the firm's shareholders than would a large base salary. As is well known by now, these high-powered incentives have, in recent years, prompted a small minority of corporate CEOs to cheat by falsifying their accounting. But far more broadly, they have enticed honest CEOs to gamble imprudently with (mostly) other people's money, because it makes sense within these pay structures to play for unlimited upside while—at least in terms of compensation—there is a floor to downside risk.

to harvest enhanced compensation for increased profits today at the expense of large risks for the corporation tomorrow.[107] Moreover, the CEO is a single person. Risk management can be enhanced through diversity in perspectives and expertise.[108] Therefore, the CEO is not the optimal center for all risk management, even if CEO input is essential for any kind of meaningful risk management.

This concept has been highlighted by recent scandals and episodes of risk mismanagement. For example, in the past few years, some CEOs have demonstrated an inclination to manipulate the system of corporate governance to harvest illegitimate gains by backdating options grants.[109] Indeed, the pervasiveness of this practice suggests that CEOs are sorely tempted by the fruits of higher compensation to expose the corporation itself to huge losses in the long term from lost investor confidence.[110] Similarly, CEOs seemed too inclined to manipulate the audit function in order to enhance their compensation (to the long term detriment and even destruction of the corporation) in the late 1990s and earlier part of this century, leading to a parade of corporate scandals.[111]

Congress responded to these risks in 2002 with the promulgation of the Sarbanes-Oxley Act ("SOX").[112] The Act imposed a new regime upon public corporations for managing the audit function.[113] Essentially, the Act stripped CEOs of power over the audit function in favor of a mandatory audit committee.[114] The Act also facilitated the creation of Qualified Legal Compliance Committees ("QLCC") [115] to

---

Andy Zelleke, *A Better Way to Pay CEOs: Smarter Incentives Could Reduce the Risks they Pursue,* CHRISTIAN SCI. MONITOR, Jan. 2, 2008, *available at* http://www.csmonitor.com/2008/0102/p09s01-coop.html.

107. *Id; see* Paul Krugman, *Banks Gone Wild,* N.Y. TIMES, Nov. 23, 2007, at A37, *available at* http://www.nytimes.com/2007/11/23/opinion/23krugman.html (describing how the system of executive compensation encourages high-risk decision making); Raghuram Rajan, *Bankers' Pay is Deeply Flawed,* FIN. TIMES, Jan. 9, 2008, at 11, *available at* http://www.ft.com/cms/s/0/18895dea-be06-11dc-8bc9-0000779fd2ac.html (noting the incentives for CEOs and financial managers to tolerate excessive risks that increase short term returns in order to receive immediate compensation).

108. *See* Ramirez, *supra* note 19, at 99 (citing evidence showing that diverse groups achieve superior cognitive outcomes).

109. Ramirez, *supra* note 105, at 345–46.

110. *Id.* at 346 n.6.

111. *See supra* notes 36–41 (describing Enron and other corporate scandals motivated by the desire for profit over investor confidence).

112. Sarbanes-Oxley Act of 2002, Pub. L. No. 107–204, 116 Stat. 745 (codified in scattered sections of 15 & 18 U.S.C.).

113. *See supra* notes 6–8 and accompanying text (describing the function and limitations of the audit requirements under the Sarbanes-Oxley Act).

114. *See supra* notes 7–9 (describing the effect of audit requirements).

115. Professor Robert Eli Rosen defines a QLCC as:

oversee the public corporation's legal compliance efforts.[116] These efforts, along with companion efforts regarding exchange listing requirements, did create positive incentives for a more appropriate framework for risk management at public corporations.[117]

Nevertheless, the Act only addressed the audit function and the legal compliance function. The legal compliance function is essentially a voluntary regime and has been implemented only at a relatively small number of public companies.[118] With respect to the audit function, SOX certainly moved the audit function away from the CEO to the board.[119] Yet, many risks escape detailed disclosure pursuant to the audit function.[120] For example, litigation risk will not generally be disclosed in a detailed fashion under prevailing audit practices.[121] Similarly, off-balance sheet transactions can still expose a company to significant, even life-threatening, risks without being discussed in a

---

> [A committee] composed of independent directors, one of whom must be a member of the audit committee. It receives and investigates reports from attorneys working for the company who have credible evidence of material violations of laws, regulations, or breaches of fiduciary duties. The QLCC makes recommendations to the entire board, the chief executive officer ("CEO"), and the general counsel or chief legal officer ("CLO"). A QLCC institutionalizes at the board level the company's responsibility to obey law.

Robert Eli Rosen, *Resistances to Reforming Corporate Governance: The Diffusion of QLCCs*, 74 FORDHAM L. REV. 1251, 1251 (2005).

116. Section 307 of SOX directed the SEC to promulgate minimum standards of professional responsibility for attorneys appearing or practicing before the SEC. In the course of imposing such standards, the SEC created the QLCC. *See* Implementation of Standards of Professional Conduct for Attorneys, 17 C.F.R. § 205 (2003) (final rule).

117. *See* Ramirez, *supra* note 105, at 355–56 (noting other federal rules of professional responsibility for attorneys "appearing or practicing before the Commission" on behalf of public companies).

118. As of late 2005, only about 2.5% of all securities issuers had adopted a QLCC. Rosen, *supra* note 115, at 1252.

119. *See supra* notes 6–8 and accompanying text (describing Sarbanes-Oxley's independent audit requirement).

120. Perhaps the best illustration of this problem is the means by which Citigroup ended up holding billions in subprime mortgage debt. Essentially, Citi sold tens of billions in collateralized debt obligations ("CDOs") that were backed by mortgage backed securities. Citi included a "liquidity put" in these CDOs which allowed investors to put these debt obligations back onto Citi's balance sheet under certain market conditions at their original cost. This provision was not included in Citi's balance sheet and was so obscure that not even Robert Rubin, the Chair of the firm's Executive Committee, knew about this risk exposure. Carol Loomis, *Robert Rubin on the Job He Never Wanted,* FORTUNE, Nov. 28, 2007, *available at* http://money.cnn.com/2007/11/09/news/newsmakers/merrill_rubin.fortune/index.htm?postversion=2007111119. Eventually, Citi announced it had $42.9 billion in such CDOs, leading to billions in losses. Roddy Boyd, *Citi's Credit Hangover,* FORTUNE, Jan. 15, 2008, *available at* http://money.cnn.com/2008/01/15/news/companies/boyd_citi.fortune/.

121. *See supra* note 17 (noting that litigation risks are not typically readily available but are relegated to footnotes in financial statements).

meaningful fashion.[122] Consequently, audit reform is not tantamount to appropriate risk management.[123]

Indeed, nothing in SOX or in other sources of corporate governance law or regulation requires that risk be systematically identified and managed across the business enterprise. Nor is there any mandate that any company center its risk management efforts at the board level or through a subcommittee of the board. Therefore, notwithstanding the SOX reform effort, risk management is still likely to be left to the discretion of the CEO.

Recent events in global financial markets demonstrate the continued inferiority of our corporate governance regime insofar as risk management is concerned. During the summer of 2007, a massive mispricing and deficient disclosure of risk emerged.[124] Specifically, rising defaults in the subprime mortgage market caused world capital markets to seize up and the largest financial institutions in the world to suffer impaired liquidity and decreased capital.[125] The uncertainty of the magnitude of subprime losses and the lack of transparency regarding which firms held the risk evolved to foment a full-fledged credit crunch and liquidity crisis in the financial sector.[126]

By the beginning of 2008, respected economists argued that a recession was inevitable; even Treasury Secretary Paulson warned of "stress and volatility" in financial markets.[127] This financial crisis had

122. Indeed, off-balance sheet risks are at the center of the current cascade of losses in the financial sector related to subprime mortgages, as financial institutions worldwide are absorbing contingent liabilities. Paul J. Davies, *AIG to Bail Out Troubled SIV,* FIN. TIMES, Jan. 23, 2008, *available at* http://www.ft.com/cms/s/0/58b3ec64-c9e1-11dc-b5dc-000077b07658.html.

123. One commentator has expressly compared Enron's off-balance sheet concealment of risk to the similarly concealed risk inherent in subprime mortgages and securities backed by subprime mortgages. *See* Bethany McLean, *Enron All Over Again,* FORTUNE, Nov. 26, 2007, *available at* http://money.cnn.com/magazines/fortune/fortune_archive/2007/11/26/101232905/index.htm (describing similarities between the Enron and subprime mortgage phenomena).

124. Krugman, *supra* note 107, at A 37 ("[T]he subprime crisis and the credit crunch are, in an important sense, the result of our failure to effectively reform corporate governance after the last set of scandals.")

125. One estimate suggests that the subprime mortgage crisis will result in restricted lending of up to $2 trillion. *Id.*

126. Lawrence Summers, *Beyond Fiscal Stimulus, More Action is Needed,* FIN. TIMES, at 9, Jan. 28, 2008, *available at* http://www.ft.com/cms/s/0/3b959570-cd41-11dc-9b2b-000077b07658.html.

127. Henry M. Paulson, Jr., U.S. Treasury Sec'y, Remarks on Housing and Capital Markets before the New York Society of Securities Analysts (Jan. 8, 2008), *available at* http://www.treasury.gov/press/releases/ hp757.htm.

its roots in the inability of market participants to manage and disclose credit risks inherent in subprime lending.[128]

Prominent economists and business publications suggest that America's broken system of corporate governance and regulation of executive compensation was central to the evolution of the subprime crisis.[129] Economist Paul Krugman asserts that executives are "lavishly rewarded" if the companies they run appear successful, even if "that success turns out to be an illusion."[130] *Fortune* magazine suggests that many of the "structured investment vehicles" that held credit risk from subprime mortgages were not disclosed on firm balance sheets—meaning these risks "were invisible to those on the outside."[131]

In other words, the same factors driving the subprime mortgage fiasco were the impetus of the corporate scandals of 2001–2002 in the period preceding Sarbanes-Oxley. Too many executives again "harvested" gains by imposing excessive risks upon their corporations.[132] Little of this excessive risk was adequately disclosed to investors.[133] In sum, SOX failed (again) to prevent major financial losses and a precipitous loss of investor confidence.[134]

IV. REGULATION AND RISK MANAGEMENT

Our system of corporate governance is flawed. It is now apparent that CEOs may exploit excessive autonomy to impose excessive long term risks on their firms in the name of greater profits and compensation today. This Part seeks to articulate a means of addressing this shortcoming with a specific focus on risk management.

One possible approach to the problem identified above would be to mimic the SOX approach with respect to audit committees.[135]

---

128. *See The Long and the Short of It,* ECONOMIST, Aug. 30, 2007 *available at* http://www.economist.com/finance/displaystory.cfm?story_id=9725837.

129. *See* Rajan, *supra* note 107, at A11 (arguing that "compensation structures that reward managers for profits, but do not claw these rewards back when losses materialize, encourage the creation of . . . more risk than we bargain for").

130. Krugman, *supra* note 107, at A37.

131. McLean, *supra* note 123.

132. Ramirez, *supra* note 105, at 346 n.5.

133. *Id.*

134. For other failures of the SOX regime, see Ramirez, *supra* note 105, at 366, 391 n.291 (discussing backdating investigations and the Refco public offering in which the CEO concealed $430 million in debts owned).

135. It is noteworthy that not all of the SOX reforms are supported with empirical data, and many commentators suggest that the law was hastily enacted and is too costly. *E.g.,* HENRY L. BUTLER & LARRY E. RIBSTEIN, THE SARBANES-OXLEY DEBACLE 3 (2006) (concluding that SOX was a costly mistake); Roberta Romano, *The Sarbanes-Oxley Act and the Making of Quack*

Essentially, SOX proscribed CEO autonomy in the specific context of the audit function and transferred that power to the audit committee which for the first time became statutorily mandated.[136] SOX imposed expertise requirements upon the audit committee or alternatively required issuers to explain the absence of such an expert.[137] In addition, SOX endowed the audit committee with new powers including ultimate control of the audit function and supervision of the auditors of public companies.[138] SOX also provided for federal regulation of the auditors and created a new regulatory agency, the Public Company Accounting Oversight Board, to oversee that regulation.[139] In the end, SOX terminated CEO (or the CEO's underling, the CFO) control of the audit function.

We do not favor this degree of intrusion into corporate governance law and regulation in the name of enterprise-wide risk management. First, unlike the audit function, there is little need for uniformity in risk management.[140] Different businesses have different risk profiles and therefore different needs for fulfilling optimal risk management.[141] Second, risk management is evolving in a healthy direction, at least at some firms, and government influence seems unlikely to foster this positive evolution.[142] Third, because enterprise-wide risk management is still in its infancy, the empirical data currently does not support an intrusive government role.[143] Simply stated, the best means of managing the risks of any particular business are not known with certainty.

Nevertheless, we do argue in favor of a mandatory qualitative disclosure to public investors of each firm's enterprise risk management approach. Given the record of enterprise-wide risk management,

---

Corporate Governance, 114 YALE L. J. 1521 (2005) (describing the political economy of the corporate governance mandates of SOX).

136. *See generally* Subcommittee on the Annual Review, *Annual Review of Federal Securities Regulation,* 58 BUS. LAW. 747, 749–50 (2003) (indicating that directors will have more responsibilities and, therefore, need broader expertise).

137. Sarbanes-Oxley Act § 407, 15 U.S.C. § 7265(a), (b) (2002).

138. *See id.* §§ 204, 301, 15 U.S.C.A. §§ 78j–1(k), (m) (vesting control over the audit function in an independent committee of the board for publicly held companies). An independent director may not receive any compensation from the issuer other than board fees and may not otherwise be affiliated with the issuer. *Id.* § 301, 15 U.S.C.A. § 78j–1(m).

139. *See* 15 U.S.C. § 7211 (Supp. III 2003) (mandating the creation of the Public Company Accounting Oversight Board ("PCAOB") to supervise auditors of publicly traded corporations). Notably, the PCAOB is subject to the plenary power of the SEC. *Id.* § 7217.

140. *See supra* Part II (describing the development of ERM).

141. *Id.*

142. *Id.*

143. *Id.*

investors have a right to know the elements of enterprise-wide risk management that a given firm has implemented.[144] Firms should be required to provide qualitative disclosures regarding their approach to enterprise risk management including: 1) whether there is a comprehensive enterprise-wide risk management function; 2) the extent of board involvement in that function; 3) whether the CEO controls that function; 4) the breadth of expertise available to address firm risks; and 5) any differences between management and risk managers regarding the firm's current risk profile.[145] This approach to the intersection of corporate governance and enterprise-wide risk management is fully consonant with the SEC's traditional role in issuing interpretative guidance.[146]

The SEC has previously utilized this very approach as a means of facilitating positive consideration of important and evolving issues in the past. During the 1970s, the SEC issued guidance regarding energy related concerns.[147] In 1998, the SEC took similar action with regard to the so-called "Y2K" challenges.[148]

It would appear that the intersection of enterprise-wide risk management and corporate governance is on par in terms of macroeconomic consequences with either Y2K or the energy crisis. The subprime mortgage catastrophe and its impact on world credit and financial markets proves that systemic mispricing of risks can have significant macroeconomic consequences.[149] In time, it could well be that the massive mispricing of risk is more likely than other factors to lead to a macroeconomic downturn. Given the stakes of enterprise-wide risk management, it poses a stronger case for such a disclosure mandate.

144. *See supra* notes 100–105 and accompanying text (noting the tested benefits of ERM and its key elements).

145. *See supra* Part III (describing the shortcomings of SOX and the rebirth of problems it was designed to prevent).

146. *See* Elliot J. Weiss, *Disclosure and Corporate Accountability*, 34 BUS. LAW. 575, 575 (1979) ("One of the central themes of the system by which large corporations are governed is that corporate decision making is regulated through mandatory disclosure requirements rather than direct government intervention.").

147. *See* Disclosure of the Impact of Possible Fuel Shortages on the Operation of Issuers Subject to the Registration and Reporting Provisions of the Federal Securities Laws, Exchange Act Release Nos. 33–5447, 34–10569, 3 SEC Docket 249 (Dec. 20, 1973) (noting the importance of prompt and accurate disclosure of information from publicly held energy companies during the fuel crisis).

148. *See* Statement of the Commission Regarding Disclosure of Year 2000 Issues and Consequences, Exchange Act Release Nos. 33–7558, 34–40277, 67 SEC Docket 1437 (July 29, 1998) (issuing guidance for disclosure of Y2K issues).

149. *See* Soros, *supra* note 10 (describing the widespread impact of the subprime mortgage lending crisis).

It is notable that SEC interpretative guidance could also operate to reduce litigation risk. The common law definition of materiality is broad and flexible. The standard of materiality is whether a reasonable investor would find a given fact important to an investment decision.[150] If this broad standard is met in a particular case, then the facts at issue become material facts which must be disclosed by public companies.[151] There are numerous cases where risk management (or mismanagement) has had profound effects on business fortunes.[152] Thus, the alternative to SEC interpretative guidance may well be decisions of the courts finding that risk management disclosures are material; the problem with this judicial assessment is that it is always inherently based upon hindsight.

In sum, we believe that our approach balances positive benefits from disclosure against *de minimus* regulatory burdens and costs, while facilitating further consideration of sophisticated enterprise-wide risk management learning.

V. CONCLUSION

Corporate governance law does not presently include any particular guidance regarding enterprise-wide risk management. Yet, enterprise-wide risk management seems to be a material element of financial performance, as a matter of logic and preliminary empirical data. Risk mismanagement can have a serious adverse effect on a business. More importantly, systemic risk mismanagement can have macroeconomic impact, as we have learned from the credit crisis of 2007–2008. Consequently, it seems appropriate for the SEC to promulgate interpretative guidance to both facilitate more optimal risk management for public companies and to limit the risk of judicial definition of the materiality of enterprise-wide risk management.

150. *See* TSC Industries, Inc. v. Northway, 426 U.S. 438, 439 (1976) (stating that the general standard of materiality is whether there is a "substantial likelihood" that a reasonable investor would consider the fact "important" in making an investment decision).

151. *Id.*

152. *See, e.g., supra* notes 14, 24–25, 36 and accompanying text (discussing the Texaco, Barings Bank, and Enron scandals).