The new model of governance and risk management for financial institutions

Received (in revised form): 28th July, 2011

John Bugalla
is Managing Principal of ermINSIGHTS, an enterprise risk management (ERM) consulting firm.

James Kallman
is a professor of finance at St Edward's University, Austin, Texas.

Steve Lindo
is Director of Treasury Management and Mortgage Risk at Fifth Third Bank, Cincinnati.

Kristina Narvaez*
is President and CEO of ERM Strategies, an enterprise risk management consulting firm.

*ERM Strategies, LLC, 9952 North 4500 West, Cedar Hills, Utah 84062, USA
Tel: +1 (801) 492 3933; E-mail: kristina@erm-strategies.com

Abstract The paper proposes a new model of governance and risk management consisting of four components: (i) board risk oversight responsibilities, (ii) a board level risk committee, (iii) an executive risk committee and (iv) an individual with responsibility for overall risk management. Some companies are subject to the Dodd–Frank Act and are forming a stand-alone risk committee; other companies still have the option of adopting these best practices. The paper contends that the new model promotes greater risk disclosure, the audit committee should complement the risk management committee, the board level risk committee should have an independent member with extensive risk management experience, the board should develop a clear risk position, management should form an executive risk committee, have a chief risk officer, create an internal risk intelligence function and, if these are done, institutions will enjoy higher stock prices.

Keywords: *risk management, Dodd–Frank, disclosure, responsibility, risk committee, risk position, chief risk officer*

INTRODUCTION

The Dodd–Frank Street Reform and Consumer Protection Act[1] (Dodd–Frank, or the Act) is squarely aimed at larger financial institutions; its objective is reforming some of the risk management efforts traditionally practised on Wall Street. One of the potentially far-reaching elements contained within Dodd–Frank (Section 165) is the requirement for a board level risk committee with one of its members being a risk 'management expert ...'. Considered in conjunction with

Securities & Exchange Commission (SEC) Rule 33-9089, the two major regulatory responses and the FCIC report provide a practical new model of governance and risk management that is needed within the financial institution community. The need for a new governance and risk model arises because banks have: (1) become highly inter-dependent; (2) built risk portfolios that are composed of complex financial instruments; (3) risk concentrations within their portfolios that are far more correlated to each other than previously considered; (4) aggregate accumulations susceptible to a high degree of both volatility and velocity; (5) traditionally managed in individual functional silos; and (6) a risk culture that incentivises risk-taking, not risk management.

In this paper the authors contend:

- The new regulations promote and provide the opportunity for greater disclosure about the risk oversight responsibilities by the board.
- The new regulations provide a structural model via a stand-alone risk committee that can be implemented by all publicly traded companies.
- The board should adopt enterprise risk management (ERM) as the ground level process to practise overall strategic risk management.
- The audit committee and the risk management committee should complement and collaborate, but not compete, with each other.
- The composition of the board level risk committee should have at least one independent member with extensive risk management experience.
- The board should work in concert with management to develop a clear description of their risk position — its risk appetite for new projects and risk tolerances for losses.
- Executive management should form a high level executive risk committee comprising members of the 'C' suite who are responsible for risk management.
- A chief risk officer (CRO) or a person with CRO responsibilities should chair the executive risk committee and should report to the board risk committee.
- One of the executive risk committee mandates should be the formation of an internal risk intelligence function to provide it and the board with information necessary for critical decision making.
- Financial institutions that successfully adopt the new model of governance and risk management coupled with superior management and strategy will enjoy a higher stock price than those that do not.

BACKGROUND

Risk management was elevated to the board agenda by the SEC amended rule 33-9089 and the 2010 Wall Street Reform and Consumer Protection Act (Dodd–Frank). A host of tell-all business books have reached best seller status by detailing the failure of governance and risk management, and that failure's impact on the financial crisis. The 2011 Financial Crisis Inquiry Commission (FCIC) report not only confirms why risk management needs to be on the board agenda, but also provides the reasons why the board has the responsibility to be actively engaged in risk oversight.[2] The report also confirms why boards should adopt a new model of governance that

includes an enterprise approach to risk management.

Two calamitous events, the financial meltdown and the Gulf oil spill, are examples of failed governance, excessive risk-taking and inadequate risk management. Two commissions (the FCIC and the National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling) were convened to examine various aspects of both events. The conclusions of both reports are the starting point of this paper.

Findings from the Commission's investigation of the BP oil spill

Below are the major findings as reported by National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling:[3]

(1) The explosive loss of the Macondo well could have been prevented.

(2) The immediate causes of the Macondo well blowout can be traced to a series of identifiable mistakes made by BP, Halliburton, and Transocean that reveal such systematic failures in risk management that they place in doubt the safety culture of the entire industry.

(3) Deepwater energy exploration and production, particularly at the frontiers of experience, involve risks for which neither industry nor government has been adequately prepared, but for which they can and must be prepared in the future.

(4) To assure human safety and environmental protection, regulatory oversight of leasing, energy exploration, and production require reforms even beyond those significant reforms already initiated since Deepwater Horizon disaster. Fundamental reform will be needed in both the structure of those in charge of regulatory oversight and their internal decision-making process to ensure their political autonomy, technical expertise and their full consideration of environmental protection concerns.

(5) Because regulatory oversight alone will not be sufficient to ensure adequate safety, the oil, and gas industry will need to take its own, unilateral steps to increase safety dramatically throughout the industry, including self-policing mechanisms that supplement governmental enforcement.

(6) The technology, laws, regulations, and practices for containing, responding to, and cleaning up spills lag behind the real risks associated with deepwater drilling into large, high-pressure reservoirs of oil and gas located far offshore and thousands of feet below the ocean's surface. Government must close the existing gap and industry must support rather than resist that effort.

Financial Crisis Inquiry Commission Findings

Below are the major findings as reported by the FCIC:[4]

(1) We conclude this financial crisis was avoidable. The crisis was the result of human action and inaction, not of Mother Nature or computer models gone haywire. The captains of finance and the public stewards of the financial system ignored warnings and failed to question, understand, and manage evolving risks within a system essential

to the well-being of the American public.

(2) We conclude widespread failure in financial regulation and supervision proved devastating to the stability of the nation's financial markets. More than thirty years of deregulation and reliance on self-regulation by financial institutions had stripped away key safeguards, which could have helped avoid catastrophe.

(3) We conclude dramatic failures of corporate governance and risk management at many systemically important financial institutions were a key cause of this crisis. There was a view that instincts for self-preservation inside major financial firms would shield them from fatal risk-taking without the need for a steady regulatory hand, which, the firms argued, would stifle innovation. Too many of these institutions acted recklessly taking on too much risk, with too little capital, and with too much dependence on short-term funding.

(4) We conclude a combination of excessive borrowing, risky investments and lack of transparency put the financial system on a collision course with crisis. Clearly, this vulnerability was related to failures of corporate governance and regulation, but it is significant enough by itself to warrant our attention here.

(5) We conclude the government was ill prepared for the crisis, and its inconsistent response added to the uncertainty and panic in the financial markets. As our report shows, key policy makers — The Treasury Department, the Federal Reserve Board, and the Federal Reserve Bank of New York — who were best positioned to watch over our markets were ill prepared for the events of 2007 and 2008.

(6) We conclude there was a systemic breakdown in accountability and ethics. The integrity of our financial markets and the public trust in those markets are essential to the economic well-being of our nation. The soundness and sustained prosperity of the financial system and our economy rely on the notions of fair dealing, responsibility, and transparency. In our economy, we expect businesses and individuals to pursue profits, at the same time that they produce products and services of quality and conduct themselves well.

(7) We conclude collapsing mortgage-lending standards and the mortgage securitization pipeline lit and spread the flame of contagion and crisis. Many mortgage lenders set the bar so low that lenders simply took eager borrowers' qualifications on faith, often with a willful disregard for a borrower's ability to pay ....

(8) We conclude the failures of credit rating agencies were essential cogs in the wheel of financial destruction. The three credit rating agencies were key enablers of the financial meltdown. The mortgage related securities at the heart of the crisis could not have been marketed and sold without their seal of approval. Investors relied on them, often blindly. In some cases, they were obligated to use them, or regulatory capital standards were hinged on them. The crisis could not have happened without the rating agencies. Their ratings helped the market soar and their downgrades through 2007 and 2008 wreaked havoc across markets and firms.

NEW REGULATION EFFECTS

SEC rule 33-9089, 'Proxy Disclosure Enhancements',[5] was effective 28th February, 2010; this rule calls for disclosure about the board's risk oversight. The disclosures in selected 2010 Fortune 1000 company corporate proxy statements indicate that an assortment of risk management approaches are being taken. There is also a variety of board committees involved with carrying out their responsibilities. Leading companies seem to disclose in their Form 14As far more information than previously about the board's risk oversight. This is in keeping with the spirit and original intent expressed by the SEC. The authors believe an example of good disclosure is to reveal any practices that present material risks to the company's shareholders. 'To reveal' means to tell with reasonable detail and in a reasonable time. 'Material' means that the risk creates sufficient volatility in outcomes that the shareholder might modify their stock ownership position. 'Risk' means an event in which the outcome is uncertain and there is significant deviation from that outcome over a planned time horizon. A specific example is when a corporation purchases derivative options as an investment vehicle to speculate on the economy. It is well understood that speculating on options is a highly volatile (risky) undertaking. This intentional taking of high risk financial instruments may represent a 'material' 'risk' to the firm's current stockholders. The authors hold that the SEC Proxy Disclosure Enhancements rule would require the above firm to promptly disclose to shareholders that the firm is using investors' capital in such a risky project.

A STRUCTURAL MODEL

The Dodd–Frank Wall Street Reform and Consumer Protection Act[1] (Dodd–Frank, or the Act) contains several key components which the authors believe will have long range implications with regard to the practice of risk management in financial institutions. Before the Act's final implementation in 2012, various studies called for in the Act must be completed. Thus the rules necessary to carry out the Act's requirements will take time to develop.

The first key Dodd–Frank component mandates the formation of a board level risk committee. The statutory requirement is aimed at financial bank holding companies, publicly-traded, non-bank financial companies, and other systemically important publicly-traded companies with more than US$10bn in assets. Dodd–Frank, however, also provides the authority to extend and expand its risk committee mandate to additional smaller or non-publicly traded financial institutions.

Various other pieces of legislation have been introduced such as the Shareholder Bill of Rights Act and the Shareholder Empowerment Act that contain a requirement for board level risk committees at all publicly-traded companies. Board level risk committees, while not yet common, are already in place at several publicly-traded financial institutions. Examples include companies such as Goldman Sachs, JPMorgan Chase (JPMC), CitiGroup, Bank of America, Morgan Stanley, Hartford, Travelers, AIG, Fannie Mae, Freddy Mac and TIAA-Creff. All of the above listed companies are in the top 100 in the USA and each company has posted their risk committee charter on

line. One board level risk committee example is found at JPMorgan Chase's web site,[6] which provides the following information:

Mission

The Risk Policy Committee is responsible for oversight of the CEO's and senior management's responsibilities to assess and manage the corporation's credit risk, market risk, interest rate risk, investment risk, liquidity risk and reputational risk, and is also responsible for review of the corporation's fiduciary and asset management activities.

Authorities and responsibilities

... In performing this oversight, the Risk Policy Committee shall:

- review with management guidelines and policies to govern the process for assessing and managing risks.
- review benchmarks for major financial risk exposure from such risks.
- receive and review reports from management of the steps it has taken to monitor and control such exposures.
- review management's performance against these policies and benchmarks.
- receive and review reports on selected risk topics as management deems appropriate from time to time.
- review the corporation's capital allocation.
- review reports of significant issues prepared by internal risk oversight functional groups.

The Committee is also responsible for oversight of the corporation's fiduciary and asset management activities, and in that capacity it reviews the oversight structure for fiduciary activities, reviews general policies and receives reports regarding these activities.

The Risk Policy Committee shall review, at least annually, the committee's charter and recommend any proposed changes to the Board for approval. The Risk Policy Committee shall prepare, and report to the Board the results of, an annual performance evaluation of the committee, which shall compare the performance of the committee with the requirements of this charter.

For comparison, consider the charter for the Finance and Risk Committee of General Motors.[7]

Risk assessment and risk management are the responsibility of the Company's management. The Committee's responsibility in this regard is one of oversight and review. Specifically, the Committee shall:

- Review with management the Company's risk appetite and risk tolerance, the ways in which risk is measured on an aggregate, company-wide basis, and the setting of aggregate and individual risk limits (quantitative and qualitative, as appropriate) and the actions taken if those limits are exceeded;
- Review with management the categories of risk the Company faces, including any risk concentrations and risk interrelationships, as well as the likelihood of occurrence and the potential impact of those risks and mitigating measures;
- Review with management the design of the Company's risk management functions including potential coverage gaps and reporting lines of authority, to assess whether they are appropriate given

the Company's size and scope of operations;
- Review management's implementation of its risk policies and procedures to assess their effectiveness;
- Review internal systems of formal and informal communication across business units and control functions to encourage the prompt and coherent flow of risk-related information and, as needed, escalation of information to management (and to the Committee and Board as appropriate); and
- Review reports from management, independent auditors, internal auditors, legal counsel, regulators, stock analysts and outside experts as considered appropriate regarding risks the Company faces and the Company's risk management function.

As the above two examples illustrate, the Risk Committee charter should contain a purpose, mission and policy provisions specific to the organisation. Boards have a legal duty of loyalty, care and disclosure to their principals (stockholders). The duty of loyalty means that boards must consider the stockholders' goals and aggregate risk position in managing the organisation's risks. A board that fails to clearly articulate these goals and risk position could be in breach of that fiduciary duty. The duty of care means that boards must exercise due diligence in adopting, participating in and enforcing ERM at all levels of the organisation's activities. The failure to have a risk committee at the board level may be an indication of a systemic breach of their fiduciary duty of care. The duty of disclosure means that boards must have regular and thorough reports to key stakeholders (including regulators and shareholders) that reveal how the ERM system identifies and manages all risks. The failure to be transparent can be interpreted as a breach of the board's duty of disclosure.

THE BOARD SHOULD ADOPT ERM

The second key component of Dodd–Frank states that a risk committee is 'responsible for the oversight of the enterprise-wide risk management practices . . . .' (p. 133) This element of the legislation can be viewed as a mandate for practicing ERM and could drive companies not already doing so to now adopt ERM. A review of 2010 proxy statements indicates that a majority of publicly-traded companies within the survey are adopting some form of ERM to serve as the process to manage risks across the entire business enterprise.

The authors recommend that financial institutions not required by Dodd–Frank to constitute a risk committee or adopt some form of ERM should aggressively do so. At a minimum, ERM can be practised with the limited function of protecting the organisation from the downside of risk. The greatest value, however, is derived when ERM is viewed and practised as a necessary component of strategic development to take advantage of the upside of risk. Various surveys taken from 2008–2010 suggest that few companies are practising risk management at the strategic level. One proposed reason is that many ERM programmes are grounded in audit and compliance. While not minimising the value of those functions, they are not necessarily strategic activities designed to add value for the business. They are usually a control function designed to protect business value. The authors' own search for examples of companies

deploying ERM strategically reveals few contenders, suggesting that those which do are choosing not to publicise the competitive advantage which they derive from it.

THE AUDIT COMMITTEE AND RISK MANAGEMENT COMMITTEES SHOULD COLLABORATE

Not adopting the recommended new model may result in the existing audit committee having primary responsibility for risk management. The authors believe this removes auditors from their essential position of independence. The board's failure to have a board level risk committee moves the auditors from their role as monitors of risk to managers of risk. The result is analogous to the fox watching the hen house. Effective outcome assessment, a key role of auditors, is compromised.

Instead, the authors recommend[8] that the all-important role of auditors remains independent from risk management so as to preserve their ability to provide unbiased and independent assessments of a firm's ERM programme. Indeed, the SEC Policy Statement: 'Establishment and Improvement of Standards Related to Auditor Independence', provides recommendations that 'maintaining the independence of auditors is crucial to the credibility of financial reporting and, in turn, the capital formation process'.[9]

The authors concur that a board's risk committee should be independent of the audit committee.[10] This separation of duties provides the protection against fiduciary malfeasance. A risk committee should lead the corporation in:

(1) the articulation of the firm's values,
(2) clearly communicating the firm's long-term strategic goals,
(3) precisely conveying the firm's risk position (both risk tolerance and risk appetite),
(4) assuring that an ERM system or framework is adopted and followed, and
(5) providing its managers with the responsibility, authority, accountability, resources and rewards for managing risks.

THE BOARD SHOULD HAVE A RISK MANAGEMENT EXPERT

The third component of Dodd–Frank is the requirement that the risk committee will contain a yet to be determined number of 'independent directors' with at least one member of the risk committee being a 'risk management expert with experience in identifying, assessing, and managing risk exposures of large, complex firms'. To the authors, the words 'independent directors' mean those board members who are not employees nor are they receiving any form of compensation from the organisation for any services other than their board level duties. What constitutes a risk management expert will be debated for years to come. A review of the published biographies of the individuals currently serving on board level risk committees, however, does not highlight a background in risk management. The authors hold that for a director to be qualified as a 'risk management expert' that individual should have not only technical training and experience in industry-standard risk management practices such as ERM but also a demonstrated track record in

managing volatility. Experience should also be broad-based in multiple disciplines, including human resources, finance, operations and strategic management.

THE BOARD SHOULD DEVELOP A CLEAR RISK POSITION

Risk position, appetite, and tolerance are three different concepts that will significantly impact both strategic decisions and tactical applications. What makes these three concepts complex at board level is the need to clarify strategic intent and provide a broad set of guidelines for risk management. At the division or profit centre level, however, the broad guidelines may become operational constraints because of risk aggregation. The authors recommend that the board's risk position must clearly specify conditions under which the risk position is applied. The concept of a risk position (also called a risk philosophy or risk attitude) is a relatively new concept in ERM. The idea is that a board should formally adopt a stance as to how much volatility it will accept on the achievement of its goals. Because strategic goals are long-term, achieving the exact desired outcome is inherently uncertain. Instead, good risk management allows for some variation from these desired goals. Deciding exactly how much variation is acceptable is an important role for the board.

A risk position comprises two separate and distinct concepts: the risk tolerance and the risk appetite. A risk appetite is defined as a firm's willingness and ability to pay a third party in order to take on speculative new risks. An example is the ability to invest in advertising in order to sell more products. The firm is never sure of the exact amount of goods the advertising will generate, but usually the managers use risk management to determine the best case, expected case and worst case scenarios. The analysis helps determine if the variation in sales will fit within the firm's appetite for volatility in product sales. Other examples that demonstrate a risk appetite include spending on R&D, new capital assets, or investing in new employees.

In contrast, a risk tolerance is defined as a firm's willingness and ability to pay a third party in order to transfer away volatile threats. The classic example is the purchase of insurance. The firm pays a certain amount to the insurer in order to transfer away possible volatile losses. Other examples include the purchase of forward or futures contracts, swaps and other derivative products. Finally, a risk tolerance can be ascertained by evaluating a firm's insurance policy deductibles or loss retention limits. All of these examples demonstrate a firm's willingness to pay for losses up to a fixed amount; and transferring away losses after that point.

There are several, non-standardised methods to express a firm's risk position. For example, one company may be willing to spend up to, but no more than 10 per cent of their economic capital in the trading room. Other companies may exhibit an appetite for gains by taking on trades whose RAPM (risk adjusted performance measure) exceeds a certain hurdle rate (H) and for whom their tolerance for losses is controlled by a variety of limits (eg value at risk (VaR) limits or stress test limits).

AN EXECUTIVE LEVEL RISK COMMITTEE SHOULD BE FORMED

Board level risk committees are the oversight element of the new governance and risk management model. Executive risk committees are the execution component of the new model. Likely members of the executive risk committee include the chief operating officer, chief financial officer, general counsel, chief audit and compliance officers, chief strategy officer, chief information officer, chief marketing officer and chief risk officer. Not all key executives need be involved in every detail of risk management, but they should be actively managing the middle management team who will be involved in every detail.

THE EXECUTIVE RISK COMMITTEE SHOULD DEVELOP AN INTERNAL RISK INTELLIGENCE FUNCTION

Like its military counterpart, the purpose of risk intelligence is to provide senior organisational leadership and the board of directors with facts, options, assessments of those options and views as to what lies beyond the readily observable. Superior risk intelligence underlies the most effective responses and enables the most efficient deployment of resources for addressing the material and critical risks of an organisation. It provides a competitive advantage to those organisations that can understand it and employ risk intelligence effectively.

Risk intelligence is both a process and a product. It consists of the organisational ability to collect and collate data, create and interpret statistics and take advantage of information concerning risk and volatility. This is followed by decision-making that produces the most favourable outcome based on the circumstances at the time.

THE CHIEF RISK OFFICER SHOULD CHAIR THE EXECUTIVE RISK COMMITTEE AND REPORT TO THE BOARD

The chief risk officer (CRO) is a relatively recent addition to the executive suite, however, the position became entrenched in the financial institution, energy, insurance and utility sectors years before the financial crisis or the oil spill in the Gulf. There is evidence that the CRO's position has evolved into a more enterprise-wide discipline that now encompasses not only financial risks, but now all aspects of an organisation's volatility. This evolution has positioned the CRO with the ability to appreciate the entire organisation's portfolio of risks. Consequently, the authors advocate that the CRO should chair the executive level risk committee or serve as its chief of staff. The authors further recommend the CRO have dual reporting lines to both the CEO and the board level risk committee. If Dodd–Frank does serve as a model to constitute stand-alone risk committees, the CRO would most likely report to the chair of the board level risk committee or the independent director with risk management expertise.

As ERM adoption and disclosure become more common, the authors hope to have sufficient data to research the number of companies that enjoy dual reporting lines for the CRO. At present the authors hypothesise that only a small percentage have this opportunity of sharing key ERM knowledge.

FIRMS THAT ADOPT ERM WILL ENJOY HIGHER STOCK PRICES

Numerous previous studies have demonstrated the value of risk management to shareholder value.[11,12] Most conclude that firms that have robust risk management programmes usually have higher stock prices. The authors hypothesise that as more firms adopt ERM and create board and executive level risk committees that the empirical data will further support the previous studies' results: risk management creates value.

Research into stock price behaviour during and after the financial sector crisis supports this. Below is a chart of the share prices between July 2008 and February 2011 of four large and complex US financial institutions. The huge disparities in relative stock price changes cannot be explained by differences in the banks' business portfolios. Rather, it is the authors' contention that they reflect the market's perception of each bank's core competence in understanding and managing its intrinsic and extrinsic risks.

The authors believe significant research is now being conducted at many universities to test the empirical evidence that firms which have more robust risk programmes usually have higher stock prices. Likewise, the authors expect future research will reveal how many financial institutions have formed an executive level risk committee comprising members of the 'C' suite.

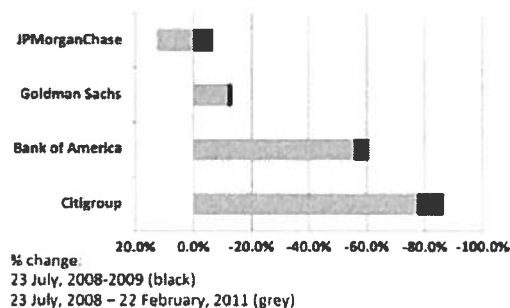

Figure 1: Major US bank's share price change: 23rd July, 2008–22nd February, 2011

CONCLUSION

The new model of governance and risk management consists of four components:

(1) risk oversight responsibilities by the board,
(2) a board level risk committee,
(3) an executive risk committee, and
(4) an individual with responsibility for overall risk management.

While companies subject to Dodd–Frank are complying with the new law and forming a stand-alone risk committee, companies not currently required by Dodd–Frank, which are the vast majority of companies in the USA – still have the option of constituting risk committees, practicing ERM, or creating a CRO position. The authors disagree with those companies who believe that their current risk management structure is already sufficiently performing risk management and that additional committee(s) add to the corporate bureaucracy and create an additional expense. Some companies are adhering to the argument that the audit committee has responsibility for issues associated with risk management and are appropriately managing risk. The authors view the audit committee mandate as assuring financial reporting integrity and determining if other controls that have been employed actually work. Internal audit should not have responsibility for risk management or risk management strategy. The authors propose that the

audit committee and the risk committee must co-exist, complement and collaborate, but operate independently under two distinct charters.

A stand-alone risk committee has the potential to bring new insights and oversee consistent risk management practices across the entire enterprise including within the strategic planning process — the corporate function where value creation is a primary goal. Investors have been shaken by the financial meltdown and the failure to practise effective risk management. Fully functioning risk committees at both the board and executive levels are a step in the right direction to gaining back shareholder confidence.

The power of ERM as a business concept is that it can be adapted to organisations of different size and complexity. When irresponsible risk-taking by the nation's largest and most complex financial institutions triggered the financial sector crisis, many smaller and less sophisticated financial institutions suffered losses. These losses could have been mitigated by proactively adopting basic ERM practices. Adjusted to suit their level of complexity, actions such as risk-position setting, having independent risk management expertise in the boardroom, and performing regular strategic reviews of changing internal and external risk factors could have not only averted catastrophic losses — but also have created enhanced shareholder value.

When financial institutions fail, the Office of Inspector General (OIG) contained within the various governmental agencies that regulate financial institutions perform examinations to determine the root causes behind the failure. An analysis of the straightforward reports indicates that most of the failures have three common elements: an inactive or complacent board, inadequate risk management and a failure by examiners.

The financial and energy sectors have employed sophisticated risk management techniques for decades; however, the risk management failures stated within both reports cited in this paper require review and corrective actions. It is the contention of this paper that both a new model of governance and risk management is the corrective model as long as it is actually practised.

References

1 'Dodd–Frank Wall Street Reform and Consumer Protection Act' (2010), available at: http://docs.house.gov/rules/finserv/ 111_hr4173_finsrvcr.pdf (accessed 19th May, 2011).

2 Financial Crisis Inquiry Commission (2011) 'The Financial Crisis Inquiry Report: Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States', US FCIC, pp. xv–xxviii, available at: http://www.gpoaccess.gov/fcic/fcic.pdf (accessed 19th May, 2011).

3 National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling (2011) 'Deepwater: The Gulf Oil Disaster and the Future of Offshore Drilling, Report to the President from the National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling', pp. vii, available at: http://www.oilspillcommission.gov/final-report (accessed 19th May, 2011).

4 Financial Crisis Inquiry Commission (2011) 'The Financial Crisis Inquiry Report: Final Report of the National Commission on the Causes of the Financial and Economic Crisis in the United States', US FCIC, pp. xvii–xxv,

available at: http://www.gpoaccess.gov/fcic/fcic.pdf (accessed 19th May, 2011).
5 Securities and Exchange Commission (2010) 'RIN 3235-AK28 proxy disclosure enhancements to 17 CFR parts 229, 239, 240, 249 and 274', available at: http://www.sec.gov/rules/final/2009/33-9089.pdf (accessed 19th May, 2011).
6 JP Morgan Chase & Co., 'Risk Policy Committee Charter', available at: http://www.jpmorganchase.com/corporate/About-JPMC/risk-committee-charter.htm#mission (accessed 19th May, 2011).
7 General Motors Company. 'Finance and Risk Committee Charter', available at: http://investor.gm.com/corporate-governance/docs/Finance_and_Risk_Committee_Charter_12-07-10_(Final).pdf (accessed 27th July, 2011).
8 Bugalla, J., Hackett, J., Kallman, J. and Narvaez, K. (2010) 'Putting board risk committees to work', *The Corporate Board*, Vol. 31, No. 185, November–December, pp. 21–25.
9 Securities and Exchange Commission (2001) 'Policy statement: Establishment and improvement of standards related to auditor independence', 17 CFR Parts 210 and 211, available at: http://www.sec.gov/rules/policy/33-7993.htm (accessed 19th May, 2011).
10 Bugalla, J., Hackett, J., McPherson, M. L. and Narvaez, K. (2010) 'Audit committees monitor control functions, risk committees provide oversight of a strategic function', BOARDMEMBER.com, 16th November, 2010.
11 McDonald, J. R. and Rivera, J. (2006) 'Enterprise risk management and improved shareholder value,' *Perspectives In Business*, St Edward's University, Austin, TX, Vol. 3, No. 1, pp. 43–49.
12 Smithson, C. (1997) 'Theory v. practice: Does financial risk management increase shareholder value?', available at: http://www.rutterassociates.com/articles/_Does%20FRM%20Increase% 20Shareholder%20Value% 20%28Risk,%20Sep96%29.htm (accessed 27th July, 2011).