Creating synergy by integrating enterprise risk management and governance

Received (in revised form): 20th November, 2008

Jean Hinrichs
recently retired from Fannie Mae as Chief Audit Executive, where she restructured internal audit and created a high-performance team during a large financial restatement. Previously, Jean was Chief Risk Officer at Barclays Global Investors (BGI) where she restructured risk management that included credit and market risk, operational risk, legal, compliance, internal audit, insurance and corporate security. She initially joined BGI in 1997 to create a global internal audit function. Jean has over 15 years' experience creating or transforming enterprise risk management and internal audit functions. She has an MBA from San Francisco State University and is a Certified Internal Auditor and Certified Fraud Examiner. She is Past President of the San Francisco Chapter of the Institute of Internal Auditors and was Co-Regional Director of the Bay Area Chapter of The Professional Risk Managers' International Association.

543–1 Green Ridge Drive, Daly City, CA 94014, USA
Tel: +1 (650) 991 1448; E-mail: thin3333@msn.com

Abstract Enterprise risk management and governance are inextricably linked to the quality and effectiveness of risk management. This paper examines the risk management weaknesses related to some recent unanticipated events in financial institutions, including specific examples related to New Century Financial, UBS and Société Générale. It also looks at how more effective integration of ERM and governance might have improved the outcomes, with a particular focus on transparency of risk exposures. Effective ERM complements governance, and good governance complements an effective ERM programme. Synergy is created when they are integrated effectively.

Keywords: *enterprise risk management, governance, transparency, New Century Financial, UBS, Société Générale, credit default swaps*

INTRODUCTION

Building effective enterprise risk management (ERM) capabilities can take years as organisations strive to find the right balance of value-added activities to manage key risks related to achieving their strategic objectives. Significant progress has been made in developing risk knowledge, skills, analytical tools and infrastructure, but challenges still remain in how to integrate all of these components effectively. The industry recently saw the dramatic decline in stock value and forced sales of Countrywide and Bear Sterns, an unprecedented $43bn loss from the subprime crisis at the Swiss banking giant UBS, and a nearly $8bn loss in unauthorised derivatives trades at the French bank Société Générale. As lack of liquidity in the market quickly became a credit crisis, many more financial institutions around the world were sold at fire-sale prices, required regulatory assistance, or failed. These

significant unanticipated events highlight either a failure of ERM or a failure of governance — or both. While there will always be some uncertainty about the future, these failures to anticipate such significant risks suggest a gap in how organisations integrate ERM and governance.

ERM and governance are inextricably linked to the quality and effectiveness of risk management. Governance establishes the strategy and policies for how business should be conducted, while ERM provides a framework for evaluating the related risks and monitoring whether the organisation is operating within that framework. The Committee of Sponsoring Organizations broadly defines ERM as:

> 'The process effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.'[1]

An often used definition of corporate governance comes from the Paris-based forum of democratic markets, the Organisation for Economic Cooperation and Development:

> 'Corporate governance involves a set of relationships between a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined.'[2]

Indicators that an organisation has integrated ERM and governance to improve the quality and effectiveness of risk management include the following:

- The strategy is clearly defined and effectively communicated.
- There is a well-defined risk framework that includes policies; delegation of authorities; processes and tools for identifying, assessing, measuring, monitoring, managing and reporting on key risks to achieving the strategy; and accountabilities.
- The management team has sufficient knowledge and experience to understand the risks and execute the strategy effectively.
- The board of directors has sufficient knowledge, experience and independence to understand and oversee the key strategic risks.
- Remuneration and incentives are aligned with strategy and a clearly-defined risk appetite.
- Performance measurement, based on appropriate industry benchmarks, is well defined and includes a balance of financial and non-financial metrics.

This paper will examine the risk management weaknesses related to some recent unanticipated events in financial institutions. It will also look at how more effective integration of ERM and governance might have improved the outcomes, with a particular focus on transparency of risk exposures.

WHY IS IT IMPORTANT TO INTEGRATE ERM AND GOVERNANCE?

ERM and governance are interdependent. ERM should focus on changes in the organisation's risk profile.

It should provide transparency regarding the critical risks inherent in the business strategy and in the execution of the business model to achieve that strategy. Governance should help balance the interests of all stakeholders using a structure that provides a system of controls and risk management to establish strategic objectives and monitor progress against achievement of those objectives. Overlap and opportunity exist to leverage setting strategic objectives, identifying and managing threats and opportunities, clarifying accountabilities and decision-making authority, and providing balanced and effective communication to stakeholders about key risks. Weak risk management policies and practices could prevent companies from identifying, measuring and managing risk effectively. Failure to set clear objectives can lead to poor business decisions, operational surprises or regulatory non-compliance.

Effective integration of ERM and governance requires a structured and well-understood risk framework. The framework should include effective policies, procedures, risk tools, assessment of results, risk aggregation and reporting, and escalation to senior management and the board. The integration of ERM and governance starts with tone at the top and cascades down through the organisation in the form of policies, procedures and management oversight. The roles of each individual and group, and each business unit or function, must be clear. ERM and governance are integrated through the activities of many people across the organisation at all levels and with the board of directors. Risk management processes and responsibilities are matrixed. They need to be integrated with effective governance practices to ensure risk taking is consistent with the organisation's risk appetite and individual authorities.

The following recent examples of risk management failures demonstrate weaknesses in the integration of ERM and governance. These organisations appear to have suffered from deficiencies in transparency of risk exposures, in addition to a host of other ERM and governance weaknesses.

New Century Financial

As New Century Financial, one of the largest subprime mortgage lenders in the USA, tried to close its books for 2007, an accounting error related to reserves for delinquent home loans was uncovered by the new CFO. This error was likely to cost New Century $300m, which was equivalent to profits from the second half of 2006. Just two months later, the firm filed for bankruptcy. New Century's collapse was the first in a series of failures among mortgage lenders. This was the tip of the iceberg that rocked global financial markets and contributed to a steep US housing market decline. Since the crisis began in 2007, financial institutions around the world have posted write-downs or losses estimated to be $400–500bn in mortgage-related securities.

A recently unsealed report by an examiner for the US Bankruptcy Court in Delaware,[3] commissioned to identify potential lawsuits in the bankruptcy case, raised several questions regarding control and governance practices. The accounting error was related to grossly understated estimates of reserves for troubled home loans. In addition, the examiner concluded that the explosive

growth at New Century exceeded the development of the firm's internal controls and policies, as well as the managerial capabilities of some key executives. The court examiner also determined that some members of New Century's board did not believe certain accounting and financial managers had sufficient acumen to run the company; one board member described the management team as 'dysfunctional', and the board questioned whether the company was being conservative and thorough enough in various aspects of its accounting. It does not appear that these concerns were acted on by the board. In addition, the examiner raised a question about the role of the external auditor regarding due professional care and consistency with Generally Accepted Accounting Principles.

Failure to integrate ERM and governance caused a lack of transparency regarding risk exposures, allowing the firm to grow faster than its risk management practices and governance. From an ERM standpoint, it appears that management did not implement basic controls such as clear policies and oversight responsibilities, or ensure that all managers were qualified to understand and manage the risks, or ensure that there were processes to monitor and report on key risk indicators in a meaningful way. Governance was ineffective because executive management and the board of directors may not have asked the right questions to make sure they understood the risks being taken. Key questions they should have asked include:

- How is New Century making money?
- Is the business model sustainable in an extreme or a declining and illiquid housing market?
- How are the risk exposures being managed?
- Does the organisation have an effective infrastructure to conduct this risk management? (For example, people, data/information, analytical tools, and management reporting and oversight.)

If these questions had been asked and the answers were both transparent and candid, New Century may have been able to improve its ERM and governance processes sufficiently early to reduce its risk exposure, thus avoiding bankruptcy.

UBS

As of April 2008, the Swiss banking giant UBS had incurred losses of $38bn since the subprime crisis began in the summer of 2007. UBS had about $3trn in assets under management. The reported losses destroyed all of its profits generated since 2004. UBS released a report to shareholders in April 2008[4] that cited an insufficiently robust risk control framework, an overly fast build-up of its investment banking activities, too much focus on maximisation of revenue growth, and a lack of clear management focus. The report indicated that UBS was using 'inappropriate risk metrics in strategic planning and risk assessments' and 'it did not react quickly enough to market changes'. The UBS CEO expanded on the findings by saying the bank had 'missed the big picture', and management 'lacked simplicity and critical perspective that prevented the right questions from being asked'.[5] The new chairman of the board of directors called for an overhaul in the management structure to clearly delineate the roles and responsibilities

between directors and executives. Continued losses and a deteriorating capital market after April 2008 led to UBS being the first Swiss financial institution to accept the support and terms of engagement from its government's rescue plan ($43bn in mortgage-related losses as of August 2008).

There were clear failures in the ERM framework and practices. Governance was compromised by the unclear roles and responsibilities of executive management and the board of directors, a lack of transparency regarding significant risk exposures, and possibly tone at the top. There was also a gap between risk taking and risk appetite because of an overwhelming focus on revenue growth.

The lack of integration between ERM and governance resulted in failure to identify and manage significant risk exposures related to growing the business without appropriate insight or controls in a changing market. The strong focus on revenue growth may have prevented senior management from sufficiently challenging one another.

The outcome might have been somewhat different had management and the board considered the following questions earlier:

- Is the approval structure for the new investment banking business, especially collateralised debt obligations, as robust as in other parts of UBS?
- Given the nature of complex structured products, is it clear what risk is transferred/sold and what risk is retained within UBS?
- Are compensation and incentives consistent with the firm's risk appetite and desired long-term results?
- Are arrangements in place to re-evaluate funding for the new business should the bank's cash capital position deteriorate?
- Are there metrics in place to benchmark growth and profitability against competitors as well as established targets?

Because the risk management framework was not sufficiently robust, the executives and directors were not informed of or failed to recognise early risk indicators that the market was deteriorating. They did not understand the impact this would have on profitability.

Société Générale

Preliminary reports on activities that contributed to a nearly $8bn loss at Société Générale due to unauthorised derivatives trading by one individual indicate a failure of basic IT access and management oversight controls, insufficient granularity in monitoring risk positions, delayed escalation of anomalies to management, and failure of senior management to react to those anomalies when escalated. According to an independent report,[6] the bank did not adequately follow up on 75 separate alerts of possible unauthorised trading by the trader between June 2006 and the beginning of 2008. The internal investigation was ultimately sparked by what appeared to be abnormal counterparty risk.

From published accounts, the ERM failure appears to have been caused in part by inadequate knowledge, experience, independence and stature of the employees in the control groups. Enquiries about trading anomalies were obfuscated or unanswered and were not escalated to senior management in a

timely manner. It has been reported by a former internal inspector at Société Générale that the traders did not take the control groups seriously and that the culture discouraged what might be perceived as interference with the traders' activities 'because they were making money for the firm'. The governance failure appears to have been caused by lack of sufficient transparency regarding the risk exposure because of inadequate monitoring and reporting, an ineffective management structure to ensure independence between the front office and control groups, and possibly tone at the top.

Failure to integrate ERM practices with governance allowed control breaches and anomalies to occur repeatedly over several years without serious challenge or escalation to senior management. When the anomalies were belatedly escalated to management, they failed to recognise the potential risk exposure and take corrective action. There are some questions that management and the board might have asked to understand the risk earlier:

- Who is responsible for monitoring trading transactions and do they have sufficient knowledge and experience to understand those transactions?
- Are potential risks being communicated to management in a balanced and compelling way?
- Does the risk organisation have sufficient credibility and stature in the organisation to be heard, and to be persuasive?

The same questions apply to oversight responsibilities, which raises another question about how differences of opinion between traders and individuals in the control functions are resolved. In short, is profitability valued more than a well controlled environment? Beyond the fundamental trading controls, a key question that should have been asked by management is how the trader could make extraordinary profits on what were supposed to be small positions. Were there sufficient metrics in place to analyse the source of the profits and benchmark them against the industry? Were remuneration and incentives rewarding the generation of profits more than the practice of prudent risk management? Without answers to these questions, management and the board of directors may not have fully understood the gap between risk taking and risk appetite at the bank.

Credit default swaps

Credit default swaps (CDS) were a key driver in the recent failure of or government intervention at several major financial institutions (eg Bear Sterns, Lehman Brothers, AIG and Merrill Lynch). CDS are derivatives that were invented in the 1990s to protect banks and bondholders from default on a particular bond or security. The seller of the CDS is required to post collateral to cover its payment obligation. CDS are complex, unregulated individual contracts that are generally not disclosed in financial statements. A decline in the value of the underlying asset triggers the need for additional collateral. As a result, the ongoing financial crisis precipitated unexpected large losses that shifted the liability for the insured securities onto the swaps' counterparties. The current market for CDS is estimated to be $45–55trn.

Insufficient integration of ERM and governance allowed certain financial institutions to assume huge, poorly

understood risks that prevented them from achieving their strategic goals — or caused them to fail completely. The lack of transparency of risks related to CDS and the failure of risk analytical models to keep pace with the explosive growth and complexity of derivatives contributed to management grossly underestimating the downside risk. Following are some examples of questions that might have helped identify the exposure earlier:

- Is stress testing sufficiently broad to identify risk exposures in an extreme or abnormal market?
- How are 'insured' risks evaluated in the overall risk profile?
- Is the measurement of potential counterparty risk comprehensive — including insurers and any fiduciaries or third-party agents?
- Do senior management and the board understand the amount of leverage involved?
- How much weight should be given to credit ratings agencies' risk assessments for structured products?
- Has scenario analysis been done to identify the interdependencies between the potential exposure, earnings, capital, liquidity, corporate credit rating, loan covenants, reputation risk and investor behaviour?
- Is executive compensation aligned with the organisation's risk appetite?

CREATING TRANSPARENCY REGARDING ONE'S LARGEST RISK EXPOSURES

If having transparency regarding significant risk exposures is so important to achieving strategic objectives, why is it difficult to get that transparency? In some cases, failure to identify or understand risk exposures stems from an ineffective risk management framework or inadequate risk assessment and measurement tools such as models. One can have similar failures in governance if the framework, tools and models are appropriate and robust, but the people using them lack the necessary skills and knowledge to interpret and report the results effectively.

In some instances, transparency regarding significant risk exposures is not possible because the strategic objectives are not clearly articulated and communicated. This can make it difficult to identify all significant risks to achieving the strategy. It can also hinder defining risk appetite and establishing specific risk tolerances.

Perhaps another reason why risks are not always transparent is because many executives think they do understand the risks. In a recent survey by Protiviti of 150 C-level executives from the largest US companies,[7] more than half of the executives surveyed thought their firms were 'very effective' at identifying and managing all potentially significant risks. The highest level of confidence came from financial services and real estate firms. Complacency may be a factor in not continuing to ask the right questions about risk. Another possibility is that financial institutions have adapted to better risk transfer by taking bigger positions, but in the process created untested liquidity risk. In some instances, the value of the instruments that effected the risk transfer was not transparent and created untested model risk.

Corporate culture may also be responsible for the lack of transparency regarding risk exposures. Risks need to be discussed broadly across the organisation to ensure all areas of risk

are considered. The right questions might not be asked because there is a reluctance to challenge colleagues, particularly those with more stature or higher positions in the firm. There may also be a fear of appearing stupid in front of colleagues.

Transparency regarding risk exposures might not be fully explored and understood at the executive and board levels due to unclear roles and responsibilities, fear of creating a roadmap of potential risks that might encourage increased shareholder and regulatory scrutiny, or concern for disclosing information that might create a competitive disadvantage for the organisation. Executives and board members may not ask the right questions to identify and understand all of the significant risk exposures because of their increased workload focused on regulatory and compliance issues and the limited time available for each agenda topic at board and committee meetings.

Effective management of the above potential deficiencies and awareness of human behaviour that could hinder communication will help improve transparency of risk exposures. Asking and understanding the answers to the three questions below will also help improve transparency.

How does the organisation make money?

It is important to start with understanding how the organisation makes money. Higher than market returns generally mean higher than average market risks. It is critical for senior management and the board of directors to understand the risk/return tradeoffs of any business activity, including the potential impact in an extreme market. Each strategic objective and any unusual significant transactions should be discussed thoroughly by executive management and the board of directors. These should be balanced discussions on the upside and downside and everything in between to ensure all significant risk exposures are understood. It is also important to agree on which risks to accept or reject.

Some companies have experienced staggering losses as a result of unanticipated events such as extreme markets, loss of investor confidence in the markets and control failures. In many cases, senior management and the board of directors did not fully understand the risk exposures, resulting in a gap between risk appetite and risk taking. There are some important questions about how the organisation makes money that would have improved transparency and decision making. First, who is responsible for making critical decisions and are they qualified? Secondly, who is responsible for oversight of critical decisions and are they at the right level to have sufficient experience and objectivity. Thirdly, how are differences of opinion resolved and at what level in the organisation?

What is your risk profile?

It is essential to understand one's risk profile, including issues such as tone at the top and the level of risk awareness in the firm's culture. Enterprise risk assessments are a primary tool used to analyse the effect and likelihood of potential future events impacting on the achievement of the organisation's business and strategic objectives within stated time horizons. This needs to be a dynamic process that compares data, metrics, information and judgment

against management's risk tolerance. An effective risk-aware culture involves having the right structure, incentives and communication to encourage behaviour consistent with the organisation's risk appetite. Going into the last decade, there were a number of risks that were not fully understood by some financial institutions, such as credit, subprime, counterparties, liquidity and consumer/investor behaviour. Failure to anticipate and incorporate these into their risk profiles caused weaknesses in risk management that led to significant losses, increased regulatory scrutiny, brand erosion and sometimes total collapse of the company.

Boards and executive management share responsibility for understanding and managing the critical risks of the organisation they lead. The CEO and board of directors are responsible for making sure continuous improvements in risk management capabilities remain a priority as the operating environment changes.

Who is accountable for results?

After assessment of the critical risk exposures, it is necessary to establish accountability for results which include:

- accepting a large risk exposure (eg continue activity);
- reducing the severity of the risk or likelihood of its occurrence (eg make operational improvements, reduce activity);
- sharing the risk with other parties (eg insurance, joint ventures);
- rejecting the risk altogether (eg discontinue a product, exit a business or market).

Accountability ensures that the risk is understood, monitored, managed and reported to the right levels of management or the board in a timely manner.

When a robust ERM framework and related processes work effectively, the chief risk officer and assurance functions are in a position to escalate knowledge and insights regarding large risk exposures. Creating an escalation process includes identifying the applicable types of activity and results, establishing timelines and levels for escalation to occur, and follow-up activities to ensure the information has been evaluated for possible adjustments in risk processes or mitigation of risk exposures. Senior management and the board need to have sufficient information to ask the necessary questions to understand how risk is being managed and who is accountable. Their questions would be similar to those listed above regarding how the organisation makes money.

CONCLUSION

Governance establishes the strategy and how business should be conducted, while ERM is a way to measure and monitor whether the organisation is operating within those defined boundaries. Integrating ERM and governance facilitates a balanced approach by ensuring that all relevant risks are considered in strategy setting, that appropriate control structures are in place, and that effective performance measures and key risk indicators are continuously monitored. There also needs to be timely and effective reporting to management and the board so that course corrections can be made along the way to stay within the organisation's risk appetite and tolerances.

A risk of not integrating ERM and governance is that risk management will fail, preventing the organisation from achieving its strategic objectives — or worse, resulting in failure of the business. An especially important component is transparency regarding significant risk exposures. There are many reasons why transparency may not be achieved, such as ineffective risk framework, policies, knowledge, skills, oversight, corporate culture or human behaviour. Transparency regarding risk exposures can be improved by understanding how the organisation makes money, understanding its risk profile, and establishing accountability for results. Asking the right questions is critical to understanding and managing significant risks. The right questions are more likely to be asked when the organisation's culture encourages robust and frequent discussions about potential risks.

Effective ERM complements governance, and good governance complements an effective ERM programme. Synergy is created when they are integrated effectively.

References

1 Committee of Sponsoring Organizations (2004) 'Enterprise Risk Management — Integrated Framework Executive Summary', available at: http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf (accessed 16th January, 2009).
2 Organisation for Economic Cooperation and Development (2004) 'OECD Principles of Corporate Governance', available at: http://www.oecd.org/document/49/O,3343,en_2649_34813_31530865_1_1_1_1,CO.html (accessed 16th January, 2009).
3 United States Bankruptcy Court for the District Delaware (2008) 'Final Report of Michael J. Missal, Bankruptcy Court Examiner', in re: New Century TRS Holdings, Inc., Chapter 11, Case No. 07-10416 (KJC), 29th February.
4 UBS (2008) 'Shareholder Report on UBS's Write-Downs', 18th April, available at: http://www.ubs.com/1/e/investors/releases.html?newsId=140339 (accessed 16th January, 2009).
5 Harnischfeger, T. and Jolly, D. (2008) 'UBS vows errant unit will get tighter rein', *New York Times*, 24th April.
6 Société Générale (2008) 'Progress Report of the Special Committee of the Board of Directors of Société Générale', 20th February, available at: http://www.sp.socgen.com/sdp/sdp.nsf/V3ID/C54C92B634428055C1257452005A7F61/$file/report%20part%201.pdf (accessed 16th January, 2009).
7 Protiviti (2007) '2007 US Risk Barometer: Survey of C-Level Executives with the Nation's Largest Companies', July, available at: http://www.protiviti.com/portal/site/pro-us/menuitem.3034b56c8d1414e79110df39f5ffbfa0 (accessed 16th January, 2009).