CELENT

Cubillas Ding

Risk Governance and the Board

Actions to Ensure a Tight Reign on Post-Crisis Business and IT Priorities

October 2009

A member of the Oliver Wyman Group

Content

Risk Governance and Failures in Risk Management

In the current climate, where there are vehement calls from political, regulatory, and investor circles for fundamental reforms to risk, compliance, and governance practices, the stakes for financial firms have never been higher. Boards and senior managers would do well to take heed and act sooner rather than later.

Recent reports and studies[1] by private and public sector authorities on the role of corporate governance in the financial crisis paid considerable attention to the issue of risk governance and, especially, the role of the board. For the financial sector in particular, most banks have given risk governance insufficient attention, and this does not only point to large multijurisdictional institutions directly involved in or affected by the crisis.

In this point of view paper, we discuss seven best practice elements. Some are to be found among the recommendations in the mentioned corporate governance studies and reports; others are not. Obviously, the ideal structures and processes for risk governance vary from one institution to another, but certain elements of best practice are common to all.

1. Reports and studies include:
   a) National Association of Corporate Directors (NACD), Key Agreed Principles to Strengthen Corporate Governance for U.S. Publicly Traded Companies, 16 October 2008.
   b) The High-level Group on Financial Supervision in the EU, chaired by Jacques de Larosière, issued its report on 25 February 2009. http://ec.europa.eu/commission_barroso/president/pdf/statement_20090225_en.pdf
   c) OECD: The Corporate Governance Lessons from the Financial Crisis, February 2009. http://www.oecd.org/dataoecd/32/1/42229620.pdf
   d) OECD: Corporate Governance and the Financial Crisis: Key Findings and Main Messages, June 2009. http://www.oecd.org/dataoecd/3/10/43056196.pdf
   e) The Walker Review: A review of corporate governance in UK banks and other financial industry entities, 16 July 2009.
   f) The Combined Code on Corporate Governance, UK, Revised June 2008.

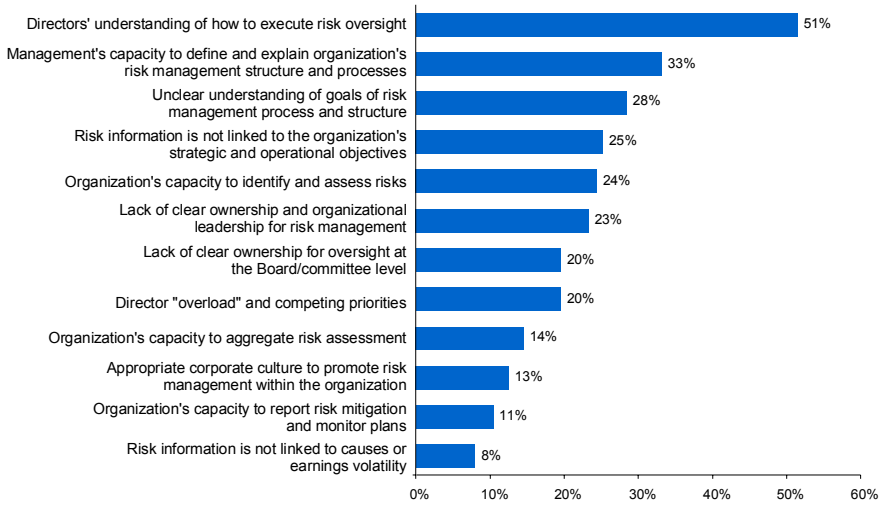
Best Practice: Strengthening the Seven Pillars of Highly Effective Risk Governance

The Board Needs Expertise and Information

Our research indicates that a bank's performance during the crisis is predicted by the degree to which its board engages with risk management. Resilient banks show much higher levels of board engagement, and have survived the crisis period without significant government intervention.

Alas, boards at too many banks are simply unable to take effective stewardship of their bank's risk profile. They frequently do not understand the risks their company faces or believe that managing them is not within their mandate, assuming the responsibility has been delegated to executive management. Indeed, at many institutions, the information that could inform them of the risk implications of business strategies or of major "off-strategy risks" is unavailable to the board.

Figure 1: Top Challenges in Providing Effective Risk Oversight



Source: National Association of Corporate Directors (NACD) / Oliver Wyman, 2009 Survey

The remedy to this malaise has two components:

- First, boards must contain greater risk expertise. Risk experts should be recruited as board members, and all board members should receive periodic risk training.

- Second, the board must be provided with appropriate risk reports. A hierarchy of reports—where the detailed report for the organisational level below serves as the appendix to the summary report for the level above—allows directors and senior managers to isolate risk issues by drilling down through the appendices. It also reassures board members that decisions made within the organisation are based on consistent and robust risk information.

Risk Appetite Should Constrain Strategy

Risk appetite should provide a genuine constraint on strategy. That is to say, the strategy must fit within a risk appetite that is decided upon independently. If the reverse is true, and risk appetite is simply fitted around a strategy, then it does no work in strategic decision-making. It is mere window dressing for a course of action that would have been adopted anyway.

Risk appetite must be set by an explicit process, requiring input from business heads, risk, finance, and the board. The risk appetite statement must specify on-strategy and off-strategy risks and give tolerance levels for all types of risk the institution faces, including capital, liquidity, earnings volatility, and reputation. Most importantly, it should be expressed in a way that can be understood and acted upon.

The ultimate test of a risk appetite statement is whether the Executive and Board of the bank would feel comfortable defending negative outcomes that are possible within its bounds. If not, the bounds have been drawn too wide.

Ensure the Independence of Risk Management

The risk function plays two important roles that require it to be appropriately independent of the business functions. It provides the businesses with assessments of risk that factor into the measurement of transaction value, customer value, and business unit performance, and it directly constrains the risk-taking of business units by setting and enforcing risk limits and by having veto power on large transactions. Both roles can be compromised by a lack of independence from the businesses.

Over recent years, the independence of the risk function at many banks has been undermined. We continue to believe that risk must be close to the business. However, reporting lines and incentive schemes must provide checks and balances that prevent risk officers from the phenomena of pseudo independence and “business capture.” Such

checks have been weakened by the common practice of giving risk managers only a dotted reporting line to the central risk function and by bonus schemes for risk managers that give them incentives to leave business volumes unchecked or to underestimate risks.

Banks that have thus tipped the balance in favour of short-term revenues must add weight to the risk management side of the scales. They can do so by addressing the operational problems associated a lack of independence and by strengthening the position of risk with the non-executive board: for example, by establishing a board risk committee and requiring board approval for hiring or firing CROs. More generally, the crisis has shown that risk committees need to be balanced between business managers and risk managers in terms of both number and seniority.

"Beef Up" the Risk Function

Risk functions can fail to bridge the gap between business acumen and quantitative expertise. Over the last decade, encouraged by the Basel II requirements, banks have built up their quantitative risk skills. However, the staff who possess these skills are rarely the experienced, traditional risk professionals who know what to look out for and who are unlikely to be "fooled by the data." Banks often find themselves with two types of risk manager: quantitative analysts, and people who understand what is being analysed from a nonquantitative standpoint.

Moreover, the understanding of fee businesses (brokerage, asset management, private banking, etc.) has historically been neglected by risk functions in favour of credit and trading operations. This is unfortunate, given that fee businesses contribute a high percentage of profits.

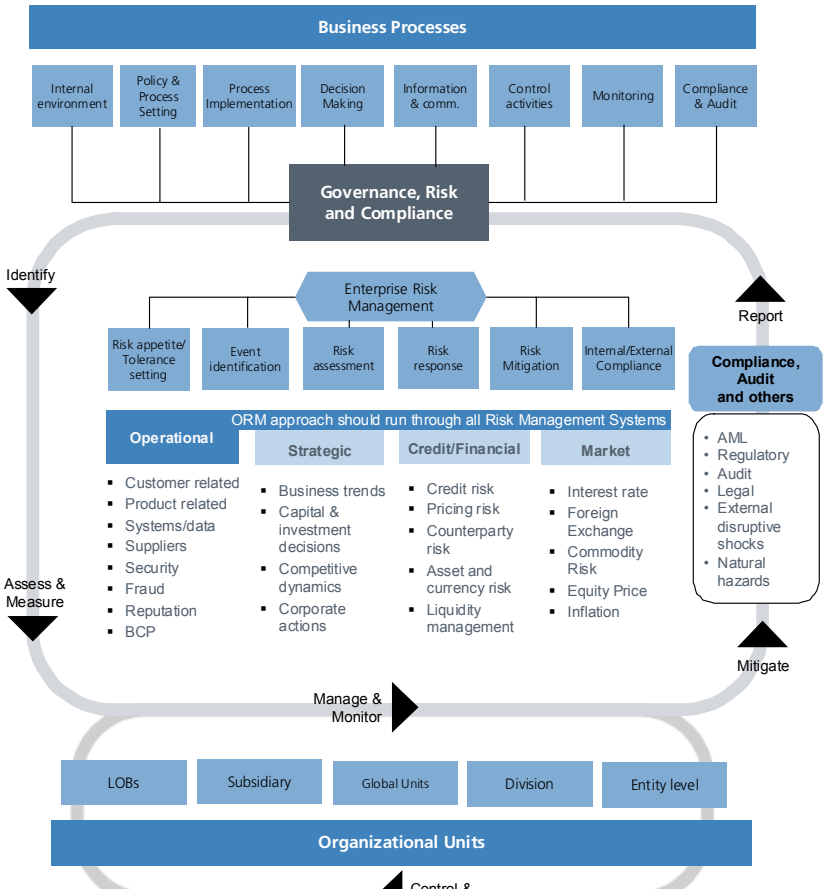
In short, high calibre risk managers who understand the risks of a wide range of businesses are in short supply. Banks must recruit and train risk managers who can become effective sparring partners for their business colleagues. This can be achieved by rotating staff between business and risk management roles, making risk experience a prerequisite for senior promotions, and ensuring a commensurate remuneration of risk professionals.

Establish a Clear and Consistent Approach to Risk Management

Banks are large, complex organisations with internal divisions of labour that reflect their individual histories and the history of the financial services industry. Risk is managed by many divisions of the bank, with a variety of concerns, processes, and data systems,

responding to a variety of regulations and internal and external customers. The risk, finance, treasury, compliance, and audit functions all contribute to the management of risk in a financial institution, as shown in Figure 2.

Figure 2: Firmwide Governance, Risk, and Compliance Model (Illustrative)



Source: Celent

Not surprisingly, there is considerable overlap in the risk-related activities of these divisions, and, with it, redundancy, inconsistency, and misalignment of priorities. For example, compliance and audit consider many of the same operational risks that risk does. But they often use different measures and rank risks according to different criteria, typically being more concerned with adherence to regulations than with the potential for catastrophic losses. Such "inconsistent overlaps" increase costs, increase the chance that risks will fall through the gaps, and can obscure senior management's line of sight to their institution's largest risks.

Many banks have responded to the growing regulatory burden by adding control processes and layers of management, increasing complexity when more simplicity is needed. Most should undergo a

review of the organisation of risk management, compliance, and audit groups, eliminating overlaps where possible, and, where impossible, ensuring that metrics, data, and priorities are at least consistent. It must be made clear who is responsible for what, what processes they will use to fulfil their responsibilities, and what data they will use and produce.

Risk-Adjusted Financial Performance Measures and Incentives

Financial institutions' compensation principles should be determined by senior management in combination with their Human Resources team, and subject to the scrutiny and approval of non-executive directors. The Institute of International Finance (IIF) has proposed a set of sensible principles, which are a good start for any bank. The following elements are most important:

- Have clear compensation governance throughout the organisation
- Use risk-adjusted performance metrics
- Demand that some compensation is put at risk against future results
- Build long-term incentive plans that manage the "trader's option" and reinforce collaborative behaviour
- Treat rule-breaking robustly, for example by eliminating bonuses or terminating contracts

Banks have often been unwilling to base incentives on risk-adjusted performance measures because they suspected the underlying risk analytics would not withstand the scrutiny of critical stakeholders. These concerns can be answered in three ways.

- First, if the risks in a portfolio really cannot be adequately determined by the risk function, then it is probably unwise to undertake this business in the first place.
- Second, there are proven techniques for incorporating checks and balances into the risk metrics that make them robust against challenge and gaming by staff.
- Third, regulators will look kindly on banks that consider the robustness of their risk adjustments when designing their bonus schemes; for example, by rewarding returns on hard-to-measure risks with deferred compensation.

Establish the Right Technology Underpinnings for Effective and Timely Risk Governance

Lastly, boards, executive management, and senior managers need to not only understand technology's role in facilitating governance processes and transparency, but also its role in posing threats to good governance.

Despite the propensity by boards and senior managers to pursue an easy option of a hands-off approach to technology, the successful experiences of forward-thinking firms with risk management and related compliance initiatives in the past decade make a strong case for cohesive risk and compliance IT approaches that are driven and executed top-down. Indeed, firmwide approaches to IT strategy formulation and a coherent IT architecture do matter significantly in the longer term. For example, anecdotal learnings from European Basel II and US SOX experiences suggest that short-sighted firms adopting departmental "band-aid" IT solutions have needed to spend more over time to meet internal and regulator expectations, hence inflicting an unnecessary drag on shareholder value.

Therefore, senior managers need to engage in partnership with IT to put in place the appropriate accountability mechanisms for technology investments to ensure the firm's overall risk governance objectives are achieved.

- Prepare an organizational response across all stages of the regulatory compliance lifecycle. A model for response to emerging legislation or ongoing regulator data calls should be developed at every stage of the regulatory cycle (i.e., from cradle to grave). With recent sweeping regulatory mandates (Basel II, Sarbanes-Oxley, Solvency II, Anti-Money Laundering), many companies responded by forming cross-functional teams working in a "SWAT team" mode that breaks down business as usual barriers and speeds implementation.

  Some examples of good practices at stages of this cycle include:

  – Setting up a multidisciplinary, compliance strategy function to act as an early warning mechanism (sponsored by the board) for impact assessment of regulations on the horizon, from a business, IT, and operational perspective.

  – Engaging in dialogue with regulatory authorities early in the legislative formation stages, especially for risk-based regulations.

- Converge fragmented risk and compliance operations. Due to the increasing burden of regulatory activities, we see best practice firms seeking convergence, optimization, and cost synergies in their risk and compliance initiatives—for example, firms consolidating control documentation spreadsheets or operational risk and compliance systems across various business lines into an integrated framework for risk-based regulatory obligations.
- Identify potential "drag areas" related to IT to future-proof emerging requirements. To identify where risks for rapid compliance with future regulations are high, for example, the IT organization should map and create schematics of all databases that contain product or customer information and the accessibility of this information to existing reporting and business intelligence tools. Areas where data is not reportable or product information is divorced from customer information should be labeled as potential drag areas for rapid compliance with future regulations, especially those that have implications for how risk is governed and managed.
- Finally, look to capture value-enhancing opportunities associated with regulations that are "risk-centric." Firms need to be in a position to capture opportunities from initiatives associated with regulatory compliance rather than merely reacting to regulation. There can be opportunities to create value associated with obligatory regulations and mandatory IT spending.
  - For example, with anti-money laundering / know your customer (AML/KYC) regulations, due to sharable procedures and data around customers and prospects, what opportunities can firms pursue to enhance customer relationship management processes?
  - For Basel II Credit Risk regulatory capital requirements, how can a firm leverage the data to develop more advanced pricing tools and sophisticated discipline around pricing, which can potentially enable firms to recapture lost loan business?

Looking Forward

Regulatory responses and corporate governance studies may spur action on risk governance. But, after recent events, no such regulatory encouragement should be required. Nor should financial institutions limit themselves to complying with regulators' requirements and recommendations. Risk governance is so fundamental to the well-being of financial institutions that they should have every reason to invest serious effort in getting it right. Table 1 provides a checklist that financial firms must address to achieve sound risk governance practices.

Table 1: Strategic Checklist for the Board and Executive Management

- Do we know which risks our business is exposed to currently and in the near future?
- How big are the key risks? Do we understand interrelationships between these risks?
- Are the risk types and magnitude in line with the firm's stakeholders' expectations?
- Am we confident that our business and risk people understand these risks?
- Are proper risk frameworks and measures in place to manage these risks?
- Are we fully informed of the key risks and their evolution with the market and changes in business mix? Are necessary events / solutions brought to our attention on a timely basis?
- Are we satisfied with interactions between my Risk and Business people? Does Risk have the expertise and authority to pull the plug when needed?
- Do we have the right risk people to support my business growth?
- Are our business and risk people properly incentivized?
- How integrated and flexible are the underlying technologies associated with the governance, risk and compliance activities?
- Is our IT adept in supporting the 'velocity' of risk taking and risk management of our business currently and in the near future?

Source: Oliver Wyman, Celent

Final Remarks

At this point, firms stand at the crossroads: put short-term fixes in place to address risk, or look towards *sustainable change*. More and more, it seems like the short-term approach is not an option, as market reforms unfold in earnest. As new realities kick in, firms need to take heed—investors, regulators, and customers are standing ready to reward firms that not only say what they do, but also can show they can do what they say. The converse is also true: the penalties for failure become higher.

In the end, by carrot or stick, firms are standing on the verge of change not only in the way risk governance practices are defined, but more importantly, in the manner that can be *demonstrably executed*. Mere theories of good governance alone are no longer sufficient.

Leveraging Celent's Expertise

If you found this report valuable, you might consider engaging with Celent for custom analysis and research. Our collective experience and the knowledge we gained while working on this report can help you streamline the creation, refinement, or execution of your strategies.

Support for Financial Institutions

Typical projects we support related to enterprise risk, operational risk, and governance include:

Vendor shortlisting and selection. We perform discovery specific to you and your business to better understand your unique needs. We then create and administer a custom RFI to selected vendors to assist you in making rapid and accurate vendor choices.

Gap analysis and business practice evaluations. We spend time evaluating your business processes, particularly in relation to risk management and compliance technology, and related data management practices. Based on our knowledge of the market, we identify potential process or technology constraints and provide clear insights that will help you implement industry best practices.

Risk and compliance IT strategy creation. We collect perspectives from your executive team, your front line business and IT staff, and your customers. We then analyze your current position, institutional capabilities, and technology against your goals. If necessary, we help you reformulate your technology and business plans to address short-term and long-term needs.

Support for Vendors

We provide services that help you refine your product and service offerings. Examples include:

Product and service strategy evaluation. We help you assess your market position in terms of functionality, technology, and services. Our strategy workshops will help you target the right customers and map your offerings to their needs.

Market messaging and collateral review. Based on our extensive experience with your potential clients, we assess your marketing and sales materials—including your website and any collateral.

Related Celent Research

Related research from Celent's Finance and Risk Service:

- *Boardroom Series: Disaster Recovery: Are You Prepared?*, September 2009
- *Enterprise Operational Risk, Compliance and Governance Solutions: Towards A Convergence End Game*, September 2009
- *Boardroom Series: US Federal Regulation of Insurance: Are We Ready?*, August 2009
- *Enterprise Risk & Governance: Trends, Vendors & Market Outlook*, June 2009
- *Commercial Lending Credit Risk Management: Surveying Business and Risk Technology Practices*, January 2009
- *Financing the Financials: Funding Trends in the New Economy*, December 2008
- *Internal Fraud: Big Brother Needs New Glasses*, November 2008
- *The New Liquidity Risk Management Paradigm: Restructuring Foundations for Best Practices*, July 2008
- *Preparing For The Credit Downturn*, June 2008
- *Model Validation Best Practices: Achieving Value-Added*, June 2008
- *Optimizing Control Functions: Achieving Lean and Solid in Meager Times*, June 2008
- *Solvency II: Overview and Impact on IT*, April 2008
- *Beyond Basel II: Evaluating the Financial & Credit Risk Solution Vendors*, April 2008
- *Managing Risk and Compliance: Responding to New Realities*, Dec 2007
- *Automated Wealth Management Compliance Solutions*, April 2007
- *Evaluating the Vendors of Anti-Money Laundering Solutions*, August 2006
- *Operational Risk Management: Three, Two, One ... Liftoff?*, May 2006
- *Operational Risk Management: Are Vendors Ready to Launch*, June 2006
- *Compliance & Technology: Best Practices for Insurers*, February 2006

Copyright Notice

Prepared by

Celent, a division of Oliver Wyman

CELENT

For more information please contact info@celent.com or:

Cubillas Ding
cding@celent.com

The author would like to acknowledge and thank the following Oliver Wyman partners and consultants for their contribution to this report - with their perspectives from a shorter version of this report published by Oliver Wyman, titled *Risk Governance: Post-crisis priorities*:

Lucas du Croo du Jong
Tom Garside
Christian Pedersen
Nick Studer

North America

USA
200 Clarendon Street, 12th Floor
Boston, Massachusetts 02116
Tel.: +1.617.262.3120
Fax: +1.617.262.3121

USA
99 Park Avenue, 5th Floor
New York, NY 10016
Tel.: +1.212.541.8100
Fax: +1.212.541.8957

USA
Four Embarcadero Center, Suite 1100
San Francisco, California 94111
Tel.: +1.415.743.7900
Fax: +1.415.743.7950

Europe

France
28, avenue Victor Hugo
75783 Paris Cedex 16
Tel.: +33.1.73.04.46.19
Fax: +33.1.45.02.30.01

United Kingdom
55 Baker Street
London W1U 8EW
Tel.: +44.20.7333.8333
Fax: +44.20.7333.8334

Asia

Japan
The Imperial Hotel Tower, 13th Floor
1-1-1 Uchisaiwai-cho
Chiyoda-ku, Tokyo 100-0011
Tel: +81.3.3596.0020
Fax: +81.3.3596.0021

China
Beijing Kerry Centre
South Tower, 15th Floor
1 Guanghua Road
Chaoyang, Beijing 100022
Tel: +86.10.8520.0350
Fax: +86.10.8520.0349

India
Golden Square Business Center
102, Eden Park, Suite 403
20, Vittal Mallya Road
Banglalore - 560 001
Tel: +91.80.22996612
Fax: +91.80.22243863