The Governance of Critical Risk
- *the new frontier in corporate governance*

Sponsored by the international insurance firm AON Global, Hong Kong

Most boards now recognize the significance of enterprise risk management. Indeed, many companies have professional risk management policies and systems, which are routinely monitored by the board. But, writes Professor Bob Tricker[1] in this paper written specifically for Aon, this may not be enough. The global financial crisis has amplified board level responsibility for corporate risk. Directors need to go beyond the management of enterprise risk towards the governance of critical risks at the strategic level.This needs to be a fundamental part of strategy formulation today. The governance of critical risk has become the new frontier for corporate governance.

Boards recognize a responsibility for risk management

The global financial crisis focused many boards on their responsibilities for recognizing and handling corporate risk. But, although risk lies at the heart of business, this recognition of boards' responsibility is relatively new. In 2004, COSO[2] of the Treadway Commission in the United States provided an integrated framework for enterprise risk management.
They explained that:

> "Enterprise risk management is a process effected by the 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 risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of

[1] Bob Tricker was founder-editor of the research journal *Corporate Governance – an international review* and wrote the first book to use the title *Corporate Governance (*1984). His most recent works are *Corporate Governance – principles, policies and practices,* Oxford University Press, 2009 and *Directors - an A-Z of corporate governance,* 5th edition of the Economist Pocket Director, Profile Books 2009

[2] Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management – Integrated Framework*, September 2004, www.coso.org, New York, NY. Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise Risk Management – Integrated Framework*, September 2004, www.coso.org, New York, NY. Originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, COSO, the Committee of Sponsoring Organizations of the Treadway Commission is a voluntary private-sector organization dedicated to guiding executive management and governance participants towards the establishment of more effective, efficient, and ethical business operations on a global basis. It sponsors and disseminates frameworks and guidance based on in-depth research, analysis, and best practices. The following organizations take part::

American Accounting Association
Institute of Management Accountants
American Institute of Certified Public Accountants
The Institute of Internal Auditors
Financial Executives International

> objectives. The challenge facing Boards is how to effectively oversee the organization's enterprise-wide risk management in a way that balances managing risks while adding value to the organization. An entity's board of directors plays a critical role in overseeing an enterprise-wide approach to risk management.

COSO's Enterprise Risk Management Integrated Framework[3] highlights four areas that contribute to board oversight of enterprise risk management:

- understand the entity's risk philosophy and concur with the entity's risk appetite
- know the extent to which management has established effective enterprise risk management of the organization
- review the entity's portfolio of risk and consider it against the entity's risk appetite
- be apprised of the most significant risks and whether management is responding appropriately

The global financial crisis put a new emphasis on corporate risk

Following the global financial crisis, proposed extensions to the Sarbanes-Oxley Act in the United States included the creation of board-level committees to focus on *enterprise risk exposure*.

Mary Schapiro, SEC Chairman U.S. Securities and Exchange Commission, said[4] in 2009:

> "The Commission will be considering whether greater disclosure is needed about how a company — and the company's board in particular — manages risks, both generally and in the context of setting compensation. I do not anticipate that we will seek to mandate any particular form of oversight; not only is this really beyond the Commission's traditional disclosure role, but it would suggest that there is a one-size-fits-all approach to risk management.

The COSO Committee published a paper in 2009 on *Effective Enterprise Risk Oversight: the Role of the Board of Directors*. It followed this with what was described as a thought paper, *Strengthening Enterprise Risk Management for Strategic Advantage,* which highlighted how boards can work with senior management to enhance risk oversight and strategic value.

The New York Stock Exchange's listing rules require audit committees of listed corporations to explain their *risk assessment and management* policies. Credit rating agencies, also, now include *enterprise risk management* processes in their corporate credit rating analysis

In 2009, Professor Jay Lorsch[5] and colleagues at the Harvard Business School interviewed directors of major US corporations about their reactions to the global financial crisis. Their

---

[3] An executive summary of COSO's *Enterprise Risk Management – Integrated Framework* provides an overview of the key principles for effective enterprise risk management and is available for free download at www.coso.org.

[4] Mary Schapiro, SEC Chairman U.S. Securities and Exchange Commission, Speech by SEC Chairman: Address to the Council of Institutional Investors, 2009 (www.sec.gov/news/speech/2009/spch040609.html).

research paper[6] argued that recent boardroom failures differed from the previous corporate failings. Enron, WorldCom and other corporate collapses were routed in management malfeasance and fraud, leading to the US Sarbanes-Oxley Act. However, recent corporate governance problems, the researchers found, were primarily attributable to the growing complexity of the companies that boards governed. The research found a strong consensus among directors that the key to improving boards' performance was not government action but action by each board and *improving risk management* was crucial.

In the UK, the Financial Review Council, considered the likely effect of the global financial crisis on the governance of companies, but failed to find evidence of serious failings in the governance of British business, outside the banking sector. However, it did propose changes to the UK Corporate Governance Code to *improve risk management.* The existing UK Combined Code, now re-named the UK Corporate Governance Code[7], includes new principles on board's *responsibility for risk management*.

In the light of the global financial crisis, the Steering Group on Corporate Governance of the OECD (the Organization for Economic Co-operation and Development) also re-examined the adequacy of their corporate governance principles, which are designed to assist countries developing their own corporate governance codes. The real need, the committee felt, was to improve the practice of the existing principles. In two seminal papers[8] *risk management* was an area identified as needing attention.

The 2010 Aon Global Enterprise Risk Management ERM Survey[9] noted that the uncertainty surrounding the global economy had significantly increased since the previous survey and that awareness of *the need to manage and leverage risk* had never been higher. Aon's five stage ERM maturity model helps organizations benchmark their progress in driving value through ERM.

The 2010 survey indicated a distinct paradigm shift as ERM has continued to evolve to an accepted and required process that provides immediate value in today's global economy. Respondents reported their level of ERM development:

38% felt that they were still at the Lacking', 'Initial' or 'Basic' level

---

[5] Professor Jay Lorsch is Louis Kirstein Professor of Human Relations at Harvard Business School, a member of the editorial board of *Corporate Governance – an international review,* and author (with Colin B. Carter) of *Back to the Drawing Board,* Harvard Business School Press 2004 and other books

[6] *Perspectives from the Boardroom 2009* – Jay Lorsch with Joe Bower, Clayton Rose, and Suraj Sriinivasan

[7] *Proposed reforms to the UK Corporate Governance Code,* FRC PN 287, 1 December 2009
For full details see http://www.frc.org.uk/corporate/reviewCombined.cfm

[8] Grant Kirkpatrick, *The Corporate Governance Lessons from the Financial Crisis,* OECD February 2009 and *Corporate Governance and the Financial Crisis: Key Findings and Main Messages,* OECD June 2009 (see www.oecd.org)

[9] *Global Enterprise Risk Management Survey 2010*, Aon Center, 200 East Randolph Street, Chicago, Ill 60601, USA. www.aon.com

55% described themselves at the 'Defined' or 'Operational' level, meaning that they had policies and techniques in place to identify, measure, and manage risk components
7% felt that they were at the 'Advanced' level, more than double since the 2007 survey

The report identified some hallmarks of advanced ERM, which included the importance of:

- board-level commitment to ERM as a critical framework for successful decision making and for driving value
- engagement of all stakeholders in the development of risk management strategy and policy setting
- a move from focusing on risk avoidance and mitigation to leveraging risk and risk management options to extract value

Levels of risk – the concept of ERM needs refining.

Corporate risk arises at a number of levels in every organization - operational, managerial, and strategic.

Operational and managerial levels of risk reflect hazards that could occur within the enterprise and from its activities. Risks at these levels are typically well-handled by ERM policies and systems. At the operational and managerial levels the directors' responsibility is to ensure that appropriate policies and control systems are in place and effective throughout the organization. The board is acting in a supervisory role, overseeing management policies, systems and performance. Many boards delegate such responsibilities to their audit committee; indeed this is recommended by some stock exchange listing rules.

Critical risk, however, is another matter. Consider the following cases:

- At Enron the board failed to understand that the company had moved beyond being a supplier of energy to a business trading in financial derivatives. In effect it had become a financial institution with a totally different risk profile. Moreover, the outside directors seemed to be unaware of the high risks their executive directors were taking.
- None of the non-executive directors at the British Northern Rock bank were bankers. The chairman was a zoologist. The executive directors, placing more emphasis on revenue generation than risk management, traded in sub-prime mortgage products. The board failed to appreciate the risks involved and the business was bailed-out by the British Government and the company nationalized.
- The Toyota car company had developed a wide-spread reputation for growth based on innovation and quality. The board built up a highly successful company using tight Japan-centered management oversight and control. Unfortunately, the directors failed to foresee the risks when they expanded the company's supply chains and manufacturing locations around the world. The price they paid was massive product recalls of entire ranges of automobile with problem brakes, steering and electronics. The cost to the company's profit was heavy: the effect on their reputation was worse.
- The board of BP plc faced a strategic catastrophe when the collapse of the Deepwater Horizon oil rig led to massive pollution in the Gulf of Mexico. The disaster, which had been treated as operational or managerial risk by the board,

had political and economic impacts that more than halved the market capitalization of the company and even put its survival at risk.

Critical risk and the crucial 'what if' questions

Taking risks is the basis of business: without risk there can be no reward. But directors need to understand the strategic risks to which their company is exposed. What are critical risks? They can be considered as any event which, should it occur, would significantly damage the company's share price or even threatened its long-term survival. BPs Deepwater Horizon oil spill reduced shareholder value by nearly 50% and Enron's debacle reduced theirs to nil.

Operational and managerial level risks can properly be delegated by the board to executive management. Critical risks lie on the board room table. They are the directors' responsibility and should not be delegated. The key question that every director should be asking is: What is our exposure to strategic risk? What if some unexpected event occurred? Every director should be constantly searching for the crucial 'what if' situation.

What if our product or service failed catastrophically? What if a major customer collapsed or changed ownership? Are we dependent on any major customers or sectors of the market? Is there any chance of a boycott by our consumers?

What if a competitor or new entrant launched a new product or service that fundamentally affected our position in the market? What if they adopted new pricing policies, or changed their distribution strategies? Could they change their supply chain or manufacturing technology to reduce costs dramatically?

What if governments, in any of the countries in which we operate, regulated our industry in a different way, introducing tariff barriers, protectionism, border controls on people, products or funds, or began monopoly or pricing inquiries? Would we be vulnerable if a government cut its procurement budget, or became politically unstable?

Information technology (IT) risk is often seen as an operational or managerial issue. But IT can pose challenging strategic risk. To what extent are our links with suppliers, customers or shareholders dependent on IT? What if the overall IT system failed? What is the possibility of hacking into our systems, spying for competitive information, attempting fraud, or maliciously damaging the firm?

The financial field can also pose significant strategic risk. What is our real exposure to off-balance sheet debt? Could predators made a hostile bid: how prepared are we if they did? What if the sources of our finance recalled their funds? Could our share price collapse if media revelations led to reputational loss?

Of course, the actual 'what if' questions depend on the industry, the markets and the company concerned. But, hopefully, the above questions will raise some relevant questions in directors' minds.

The governance of critical risk

To grow and achieve their goals, companies add value in different ways. Where value is added is where companies can be strategically exposed. In some businesses it could be the strength of the global up-stream supply chain, in others technological know-how, brand image and dominant market position, the down-stream distribution network, access to finance, managerial experience, or reputation.

Amazingly, studies have shown that some outside directors do not know where value is added in their company. Consequently, they cannot know where the company is strategically exposed to risk. Strategic risks are, potentially, the most significant that companies face. Yet they may be the least well understood by boards. In the global financial crisis it was apparent that many directors did not understand their firms' exposure to strategic risk.

Identifying and assessing critical risk should be a board level activity. The handling of operational and managerial risk can be delegated to management, whilst the board ensures that the ERM policies and systems are working. But decisions about risks at the strategic level should not be delegated. They are fundamentally part of the board's responsibility for formulating strategy. Of course, senior management play an important part in the process, but the responsibility is ultimately the boards.

The essence of successful business at the strategic level is taking business risks that satisfy customers, create employment and generate sustainable wealth. Facing critical risk, boards have four choices. They can:

1. Avoid the risk by deciding not to pursue a particular strategy, for example by deciding not to pursue a possible take-over bid
2. transfer the risk to a third party, for example through insurance, hedging, or outsourcing
3. control the risk by expenditures, such as staff training, stand-by systems, or back-up supplies
4. accept the risk to generate shareholder value. That is the way profits are generated.

Some executive incentive systems seem to encourage executives to pursue excessive strategic risks and fail to identify the company's exposure to risk. The governance of critical risk is component of professional strategy formulation and, thus, a part of corporate governance. Indeed, it has become the frontier of the subject.

Ten steps to the better governance of critical risk

So how might boards respond to this vital challenge? The following ten steps might help board chairmen guide their colleagues' deliberations.

Step 1 Ensure that all directors really understand critical risks at the strategic level
Director induction, board-level training, briefings and updates, and mentors can be useful.

Step 2 Confirm that every independent, outside directors knows where value is added in the business and therefore where the company is exposed to critical risk
Briefings from top executives and other experts may be valuable.

Step 3 Accept that the governance of critical risk is a board level responsibility

Board chairmen might consider adding decisions about strategic risk to the board policy on decisions reserved to the board that is those decisions that cannot be delegated to executive management.

Step 4 Uncouple the governance of critical risk from enterprise risk management
The board can delegate responsibility for enterprise risk management at the operational and managerial levels to their audit committee.

Step 5 Recognize that the governance of critical risk should not be delegated by the board, other than to a board critical risk committee. Even then every director needs to know where the company's strategy is exposed to strategic risk.

Step 6 Review the way the board formulate strategy and handle critical risk

Step 7 Incorporate the governance of critical risk into the board's strategy formulation process

Step 8 Have frequent board briefings on critical risk from management and outside experts

Step 9 Ensure that no strategic decision is taken by the board without a critical risk analysis

Step 10 Consider the company's overall exposure to critical risk including reputational risk and ensure that contingency systems are in place

Conclusions
Every director needs to understand where value is added in their company. Directors must appreciate the critical risks at the strategic level to which their business is exposed. Moreover, they should consider the likelihood of such risks occurring and their possible consequences. This is a crucial part of professional corporate governance and every director's duty.

Boards need to accept that the governance of critical risk is a board responsibility. It is a fundamental component of the board's corporate governance role. Every strategic decision faced by the board, whether it involves capital investment, mergers and acquisitions, or product, marketing, financial, or organizational strategies, should be searching for the crucial 'what if' situation.