

“Risk Management is Dead..., Long Live Risk Management”

How the management of risk as set out in corporate governance guidelines can benefit from Business Continuity Management practices in light of short-comings exposed in the financial crisis.

This paper is intended to stimulate robust debate on how to address the weaknesses exposed in Corporate Governance as they relate to the practice of risk management. These fault-lines are widely blamed as contributing factors to the recent economic crisis in the financial services sector.

This paper asserts that the development of a Corporate Impact Policy provides senior management with an objective and straightforward device to manage the complex environment in which they aim to deliver their corporate objectives.

Although this paper is based on analysis of the financial services sector, lessons can be learned and applied to other sectors of the economy.

Contents

Introduction 3

The financial crisis and corporate governance 3

It’s not just about the financial services sector 6

Risk management has let its supporters down..... 6

The response that will not work 8

But isn’t Business Continuity Management just part of operational risk management?..... 9

The value of Business Continuity Management in corporate governance..... 9

What are the respective roles and responsibilities of the board, board committees, auditors, key executives, employees and other that may be involved? 13

Is this enough? 14

About the Business Continuity Institute 14

Contacting the Business Continuity Institute..... 14

Introduction

Many of the financial institutions that collapsed with the credit crunch boasted robust risk management systems in their organisations and yet the systemic failure of the financial system was not widely foreseen. Some risk experts have asserted that the problem with risk management is that the focus is on high probability events, whereas the “credit crunch” was a big impact but low probability event¹. Another issue indicated in an OECD report² is that company boards lacked a clear understanding of the changing risk profile of the businesses they manage.

An American pundit once observed that politicians often read the wrong thing from election results - when the people reject "ham and eggs" the tendency of politicians is to offer "double" ham and eggs. We should therefore resist demands for “more” risk management and consider what we are trying to achieve with Corporate Governance guidelines: Corporate Governance seeks to assign accountability and deliver transparency to stakeholders, risk management has failed to deliver this.

This paper outlines how the Business Continuity Management (BCM) methodology and specifically the establishment of an Impact Policy at board-level can provide a coherent response to some of the problems experienced in risk management.

The financial crisis and corporate governance

Good corporate governance leads to financial market stability, investment and economic growth. It is an instrument of economic efficiency and investor confidence. The perceived quality of a company’s corporate governance can affect its share price and the cost of raising capital.

The financial crisis is presented as a crisis in corporate governance. It is clearly important to note that it was not entirely caused by risk management systems themselves but risk management practices have been identified along with incentive systems and internal control systems as contributors.

Understanding risk exposure is an internal control issue for executive and non-executive directors. A failure of internal control is therefore a fundamental corporate governance issue.

The presence of an effective corporate governance system within an individual company and across an economy as a whole helps to provide a degree of confidence that is necessary for the proper functioning of a market economy.

OECD’s Principles of Corporate Governance 2004.

The UK’s Institute of Directors stated³ that the credit crunch has emphasised the importance of risk management as a board-level responsibility. The role of the board is seen as three-fold:

- Evaluate risk associated with the corporate strategies.

¹ Global Risks 2009, A World Economic Forum Report, January 2009, page 11.

² Corporate Governance Lessons from the Financial Crisis, OECD 2009.

³ Risk Management and the Financial Crisis³ (February 2009), Institute of Directors.


- Define the risk appetite of the company.
- Ensure that appropriate resources are identified for risk identification, avoidance and mitigation.

The OECD's report "Corporate Governance Lessons from the Financial Crisis" February 2009 covered the shareholder report on the UBS write-downs of 2008, the causes of the \$18.7bn write-down were given as follows:

- There was no monitoring of counter-party risk
- There was no analysis of risks in the sub-prime market
- Credit rating were accepted at face value

Bear Stearns and Northern Rock both argued that the risk of liquidity drying up was not foreseen. However a US bank, Countrywide, which has subsequently been acquired by Bank of America, operated a similar business model to Northern Rock (loans through wholesale market funds and not depositors) and had put in place emergency lines of credit at some extra cost to themselves.

Some banks identified sources of significant risk as early as mid-2006, e.g. sub-prime defaults, and took measures to mitigate the risks.



"The failure to properly evaluate and challenge risk of overall business strategies was probably the biggest intellectual failure of boards, regulators and shareholders."

Lord Turner, FSA Chairman in the UK.

It is worth noting that in the BCI's case study on how Euroclear Bank weathered the collapse of Lehman Brothers in September 2008, it was a combination of pro-activity from the national regulator and the timely application of Business Continuity Management methodology that enabled this bank to respond to the crisis created by the collapse of a counter-party.

The problem has however been identified - risk issues have increasingly become too specialist for meaningful oversight by the whole board and the "tone at the top" meant that there was an unhealthy imbalance between growth and control. Understanding the changing risk profile requires the right background in finance, consultancy, risk and audit, of

course, there is a natural limit to those who can meet these requirements and this presents another reason to simplify the approach.

Where does Risk Management fit within Corporate Governance?

Within the OECD Principles for Corporate Governance risk management features heavily in two areas:

- Disclosure & Transparency

The key item here is the recommendation to disclose material information on foreseeable risk factors including disclosure on the system for monitoring and managing risk. These foreseeable risks may be industry specific, geographical, a commodity dependency, environmental liabilities,

derivatives, financial market risk such as interest rates or currency and off-balance sheet transactions.

- Responsibilities of the Board

The board is responsible for reviewing and guiding risk policy. Risk policy is seen as closely related to corporate strategy. Boards should specify the types and degree of risk that a company is willing to accept in pursuit of its goals. It must manage risk to meet the company's desired risk profile.

In 2008, KPMG reported that from their research of 150 UK audit committee members and 1,000 internationally, only 46% were very satisfied that their company had an effective process to identify the potentially significant business risks facing the company; and a lowly 35% were satisfied with the risk reports they received from management.

Corporate governance models around the world reflect these guidelines either through voluntary codes of practice, regulation or legislation. Companies outside the US have been agreeable to providing a statement on internal controls and risk management issues in the annual report but have eschewed any requirement to make a statement on effectiveness. Under the EU accounts modernisation directive 2003 and the Companies Act 2006 companies must report on non-financial issues with a Business Review in the annual report.

UK best practice is a combination of the Combined Code, Company Law and Listings rules. The UK relies on institutional investors to influence governance; whereas the US has majored on greater regulation, such as Sarbanes Oxley, as small investors form a majority component US corporate ownership. Most EU countries have followed the UK approach rather than the US model.

The Turnbull Guidance, published in 1999 in the UK, and later incorporated within the UK's Combined Code, explicitly tackles risk management. Soon after the guidance was issued, there was a lot of activity from consultants and IT software companies seeking to increase its complexity with the establishment of risk registers and systems to demonstrate to shareholders and regulators that appropriate controls and risk management policies were in place.

"It is possible that some directors may not have a good idea about what risks may affect the business when the board begins the process but the board should push to develop this understanding."

Jack Krol, Tyco International. From "Using OECD Principles of Corporate Governance – A Board Room Perspective". OECD 2008.

The UK trade-association, the Confederation of British Industry (CBI), holds the view that companies should review all risks and controls and not just those related to financial reporting and that the Turnbull approach represented a leap forward for many companies in focusing on the broader reasons why businesses fail rather than the purely financial ones.⁴

The CBI also feels that it is better if guidance is accessible for boards and managers rather than requiring the assistance in interpretation of lawyers, accountants (and other specialists). This helps to ensure that the responsibility for risk management rests where it should – with the board and management.⁴

“Risk Management is too complicated, it’s a black box, it ties hard to soft data and makes erroneous comparisons; it works against the grain of common sense. BCM is objective.

The drivers for BCM are different they are based on IMPACT and TIME. BCM focuses on things that have a big impact even with low probability whereas Risk Management identifies the risks. Risk Management looks at everything that could go wrong so it becomes complicated – and it hasn’t worked. Impact is easy to measure, risk is not.”

Lyndon Bird FBCI, The Business Continuity Institute.

Business continuity “risk” was detailed in the 1999 Turnbull Guidance. In 2005 the Financial Reporting Council tried to raise the profile of Business Continuity Management however the CBI, by way of example, rejected this saying that risks vary greatly from company to company⁴. The CBI felt it would be of more relevance to some companies than others. This clearly indicates a lack of understanding of the potential benefits of Business Continuity Management.

It’s not just about the financial services sector

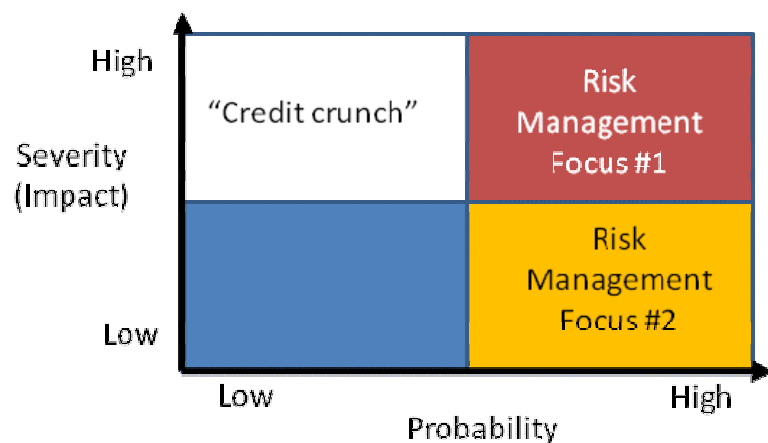
Although the catalyst to re-examine Risk Management practices has been the financial crisis, similar problems have been seen at other companies in different sectors. Moreover given the finance sector forms a part of any market economy’s critical national infrastructure, any financial crisis will have an impact on organisations in other sectors manifesting itself in the form of the withdrawal of insurance for credit lines or reduced access to capital to fund the business. Loss of access to funding and insurance, arguably akin to a supply chain failure, can now be added to the threat register alongside the loss of IT, facilities and people.

Risk management has let its supporters down

Once largely associated with insurance, compliance and loss avoidance, the risk management function has been transformed in recent years and is now firmly entrenched as a board-level concern. The traditional focus was on credit risk, market risk and foreign-exchange risk.

In 2007 the Economist Intelligence Unit’s report on “Best Practice in Risk Management, A function comes of age” stated that their Risk Barometer had tracked a change in corporate attitudes – respondents considered credit risk and foreign-exchange risk to be so low on their list of priorities due to the continuing innovation that had taken place in financial risk management. It stated that there had been “significant development in the tools to manage these more quantifiable risks, with many companies adopting hedging strategies to protect against risks such as credit defaults or swings in currency rates”.

Figure 1: An Example Risk Assessment Framework



⁴ CBI March 2005 – CBI response to the FRC Turnbull Review Group on the Review of Turnbull Guidance.

Risk Management frameworks exist – An Enterprise Risk Management (ERM) framework has been defined and one definition runs as follows “a 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 risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”⁵

In the case referenced above the ERM framework comprises eight stages:

1. *The internal environment.* This encompasses the tone of an organisation and sets the basis for how risk is viewed and addressed by an entity’s people.
2. *Objective setting:* objectives must exist before management can identify potential events affecting their achievement.
3. *Event identification:* internal and external events affecting achievement of an entity’s objectives must be identified, distinguishing between risks and opportunities.
4. *Risk assessment:* risks are analysed, considering likelihood and impact, as a basis for determining how they should be managed.
5. *Risk response:* management selects risk responses developing a set of actions to align risks with the entity’s risk tolerances and its risk appetite.
6. *Control activities:* policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
7. *Information and communication:* relevant information is identified, captured and communicated throughout the organisation in a form and timeframe that enable people to carry out their responsibilities.
8. *Monitoring:* the entirety of enterprise risk management is monitored and modifications made as necessary.

What is missing from the ERM model?

The ERM model does indeed consider an organisation’s objectives however it then steps into assessing all internal and external events that could affect achievement of these objectives. Given that ERM requires threats to be identified it can only take into account those that are known and recognised. As a result, disruptions arising from outside management’s attention – because they are new or taken for granted – will not feature in the list.

Furthermore ERM takes the ranked list of risks and then determines a response to all of them - even if that response is to ignore the risk; would it not be better to rank threats by impact and then undertakes risk assessment only for those that would carry a significant and rapid impact on the business? The former approach can clearly become complex and extremely resource intensive. It is also worth noting that ERM does not explicitly take the step of understanding the critical assets and processes that underpin the business and operating model, without this assessment how is it possible to be sure that the “risk register” is appropriate?

The ERM model stops at monitoring, whereas it would seem to make sense that exercising forms a fundamental part of the process to make sure that the planned response is workable and effective.

⁵ Committee of Sponsoring Organisations of the Treadway Commission, 2004, taken from OECD’s “The Corporate Governance Lessons from the Financial Crisis” 2009.

Analysis of the financial crisis has shown that *stress testing* has been insufficiently consistent or comprehensive in some banks. The OECD noted that “It is clear that firms need to ensure that stress testing methodologies and policies are consistently applied throughout the firm, evaluating multiple risk factors as well as multiple business units and adequately deal with correlations between different risk factors.”²

And perhaps the key area in light of the financial crisis is “culture”. For any risk management methodology to be effective it must be embedded within an organisation’s culture with “tone from the top” being matched by communication, processes and procedures throughout the organisation to ensure that all stakeholders respond in line with the organisation’s needs.

The response that will not work

It is optimistic to suggest the following “double ham and eggs” responses to the crisis in risk management⁶ will provide the remedy to the problem. The approach of more of the same but better demands that:

- Risk Management must be given greater authority
- Institutions need to review the level of risk expertise in their organisation, particularly at the highest levels.
- Institutions should pay more attention to the data that populates risk models, and must combine this output with human judgement.
- Risk factors should be consolidated across all the institution’s operations
- Risk management systems should be adaptive rather than static

When risk hides a painful truth!

In any horse race there are different odds that reflect the relative chances of each participant winning. Someone who decides to “bet the house” on the favourite or the outsider is taking a risk and the probability of winning is clearly reflected in how much can be won, however the impact of losing regardless of which horse the bet is placed upon is the same – you are homeless!

At the World Economic Forum in January 2008 the following comments were made on risk management and assessing risk:

- Risk plans need more resilience and in particular lack the kind of built-in redundancy that can alleviate total failure in interconnected systems.
- Risk plans also require better blue prints for managing a crisis as it unfolds.
- Risk plans should also carefully consider the best route towards recovery and embed in them the ability to learn and respond.
- Risk plans are ignoring the obvious due to myopia and insufficient thinking e.g. the probability that a failed terrorist attack will result in another attempt and neglecting to look at predictable natural weather patterns.

These proposed changes are in effect what Business Continuity Management already provides.

⁶ Taken from “Managing Risk in Perilous Times, Practical Steps to Accelerate the Recovery”, Economist Intelligence Unit March 2009 (edited).

But isn't Business Continuity Management just part of operational risk management?

Some risk managers have seen Business Continuity Management (BCM) as a response to a risk management issue. With this approach risk managers look at all risks and all impacts and then identify the treatments, these treatments include transferring the risk (through insurance), accepting the risk, reducing the risk or avoiding the risk, the other option is to apply Business Continuity Management.

The mistake here is that transferring the risk still leaves you with a business continuity issue if the threat is realised. Accepting the risk means going ahead with the project without taking any measures and reducing the risk may involve additional investment or scaling down ambitions. Given that the assets or processes identified for treatment have already been agreed as critical for the organisation in reality all of them require BCM treatment.

What is Business Continuity Management?

Business Continuity Management (BCM) identifies potential threats to an organisation and the potential impacts to business operations of those threats. It provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of key stakeholders, reputation, brand and value-creating activities.

It's also worth pausing to note the origins of Business Continuity Management and risk management – Business Continuity Management as a concept developed from the need to keep businesses operational, whereas risk management has effectively evolved from the insurance industry, which has advocated the need for actuarial models and complexity to avoid financial losses. In traditional risk management, risk (the loss of money) can be transferred or avoided, in reality, when the same techniques are applied to operational risk a false sense of security is created as the impacts are not just financial but are substantially intangible such as loss of reputation and long term impact of not being seen as a well run business by stakeholders.

The value of Business Continuity Management in corporate governance

This paper asserts that a different discussion is required in the board room. If the strategy and business model are set, then the real questions are to identify and agree the value creating processes within the business and any key dependencies including critical assets, customers or suppliers. Directors should then understand how the organisation is going to protect these value creating processes and in the event of a disruption question the plans for responding to and recovering from it.

The key proposal in this paper is that an Impact Policy be developed and managed at board level and become an integral part of a reformed corporate governance framework in respect of risk management.

In Figure 2 we have outlined an evolved risk management framework which could be applied within a corporate governance model.



Figure 2: A Corporate Governance framework that provides an enhanced approach to risk management.

Stage 1 - Understanding the Organisation

In this model the board will focus on corporate strategy development and understanding the business model as per today, however *prior* to any risk or threat assessment activities the board will identify and document critical processes and assets which underpin its ability to create value for its shareholders.

Stage 2 – Understanding Impacts

In the next step the question is asked “what would be the *impact* on the business if these processes failed or an asset was not available?” These questions can normally be answered without too much analysis or subjective modelling. From this analysis it is possible to identify how quickly and therefore what investment should be made to ensure that recovery and full restoration of these processes or assets occurs within timeframes sustainable by the business.

We would recommend this new focus on event impacts rather than risks or threats⁷. There are many threats but event impacts are generally limited to key processes and/or assets. Impacts can also be assessed objectively whereas threat assessments are highly subjective. From a policy perspective it is easier to detail and review event impacts rather than a list of threats with overlapping impacts, for example there are many threats which, if realised, could lead to an absence of staff. So the BCM focus is on dealing with the impact of a loss of staff, work which would be “re-usable” across many scenarios.

An event impact can be felt on one or more of the following seven areas within an organisation:

- Reputation
- Customers
- Suppliers
- Finance
- People
- Information & Communications Technology
- Sites & Facilities

Working backwards it is clearly possible to develop an approach to deal with seven impacts rather than an extensive risk/threat register with overlapping impacts. None of these impacts would be a surprise to a BCM practitioner as all except finance are the bread and butter of Business Continuity Management practice. If an event would stop key value creating processes, however remote, then surely an organisation should take steps to mitigate the impact and develop greater resiliency *or explain to shareholders why it does not take this approach*.

From this step an “Impact Policy” can be developed. This will be a clear statement from the board on the processes and assets that drive shareholder value within the business and the need to make all reasonable efforts to minimise anything that would impair their performance.

Stage 3 – Understanding Threats

Up to this point no one has been asked for any assessment of specific threats, the approach so far has been to identify and isolate what drives value in the business and agree that the company should be focused on minimising the downtime of these processes and assets.

The threat assessment phase is now focused on any threat that has an impact on business activities the loss of which would most quickly be felt - arguably devoid of any arbitrary view on probability.

Threat identification, assessment and reporting are still necessary within an organisation. Being better than competitors at detecting and understanding threats can be crucial in gaining early access to what may be limited resources when a crisis hits. The first organisation to recognise an impending crisis will get the best price on insurance, the first bite at alternative partners or the best rates on additional facilities such as warehousing or shipping.

However threat assessment needs to be made within the context of preserving the value creating processes of an enterprise as identified in the Impact Policy and sit further downstream than its current position in the process.

⁷ A paper could be written on the meaning and application of words risk, threat and hazard. In this paper we prefer the use of “threat” rather than “risk”. Both “threat” and “hazard” refer to a source of or cause of harm whereas “risk” refers to the subjective assessment of the chance or probability of a threat or hazard actually happening.

Stage 4 - Execution

The next stages are to be conducted at the specialist operational level of the organisation and will look at determining the continuity strategy and developing and implementing the response.

The final two stages in the model do require direction and investment of time and resources from the Board. There is no substitute for testing out an organisation's response plans but these tests can be expensive and time consuming, so top level support of regular testing of procedures to deal with major impact events is required. Moreover ensuring that plans and exercises reflect organisational change is vital such as following mergers, acquisitions and divestitures. *Stress testing* and related scenario-analysis are important Business Continuity Management tools.

Embedding in the Organisation

The final element effectively supports the whole framework and concerns the need to embed good practice throughout the organisation. One of the criticisms in the analysis of the financial crisis was that tone at the top established a culture of risk taking and internal control mechanisms came a poor second to the demands for growth. As Citigroup's Chief Executive, Charles O. Prince said in July 2007, *"As long as the music is playing, you've got to get up and dance. We're still dancing"*.

A further advantage with Business Continuity Management is that standards exist already and the BCI recommends, as a minimum, compliance with available standards in Business Continuity Management and in some cases organisations may choose external certification to provide an independent assessment of their approach.

What are the respective roles and responsibilities of the board, board committees, auditors, key executives, employees and other that may be involved?

Board (Non-Executive Directors) – Non-Executive Directors should understand the business model of the company and the key dependencies to maintain the business as a going concern and that the Board overall has set a policy to ensure that all reasonable efforts are being made to protect the value creating processes of the business. The board could carry out visits to see for itself; the board could ask for reports; the board could bring in independent assessors.

Board (Audit) Committee – The Audit Committee should require regular exercises to test the organisation’s commitment to the Impact Policy. At least one Non-Executive should take on responsibility for Business Continuity Management oversight in addition to Executive responsibility.

BCM helps the Executive and Non-Executive Director focus on the key questions:

1. The company’s business and operating model.
2. Key value creating products and services.
3. Key dependencies – critical assets and processes.
4. How the company will respond to a loss or threat to any of these.
5. What the main threats are today and on the horizon.
6. Evidence that the plans will work in practice.

Auditors – The auditors should look for examples of “challenge” and “questioning” by Non-Executive Directors of the Impact Policy, this would be a good opportunity to harness the varied experience of Non-Executives and counter-check for signs of “Group Think”. Auditors owe a duty of professional care to the company and not to management. This is why shareholders of the audit committee appoint them.

Key Executives – The key executive clearly understand the business model better than any of the other parties and they have the responsibility to confirm the business model and critical assets. They would also find that BCM provides an easier way to have a dialogue with the board and investors.

Employees – By its nature Business Continuity Management is cross-functional and cross Line of Business (there may well be dependencies that multiple Lines of Business (LoBs) share that are, in isolation, not seen as critical). At the operational level, we would advocate a senior level specialist, who has regular access to the Audit Committee and can provide reports, recommendations and advice to senior company Executives

Shareholders –Shareholders should ask to see evidence that this thinking and analysis has taken place and that appropriate control structures are in place to give confidence in the ability of the company to deal with major disruptions and preserve shareholder value. They need to demand transparency from the company.

Is this enough?

The failure of risk management systems was only a contributor to the financial crisis – broader issues of internal control and remuneration systems also played their part. Whatever the causes of the current crisis, this paper asserts that more complexity is not going to solve the problem. Complexity is the enemy of understanding. Companies are rushing to overhaul risk management policies and processes to provide a better overall picture of risk with the latest tools. This is just “Double Ham and Eggs” thinking.

The Business Continuity Management framework has the advantage of simplicity and provides senior management with the tools to ask the right questions. The focus on understanding the business model, its key products, services and activities and their time-criticality would appear to be a logical role for the board and core tenet of corporate governance. The development of a Corporate Impact Policy would provide a much clearer direction to the company’s underlying businesses and be easier to manage from the board.

About the Business Continuity Institute

The Business Continuity Institute (BCI) was founded in 1994 and leads on the development of best practice in Business Continuity Management (BCM). The BCI’s Good Practice Guidelines define the BCM framework. The BCI also contributes to relevant legislation and standards. It has some 4,800 members in over 80 countries active in an estimated 2,500 organisations in private, public and third sectors. The BCI Partnership, established in 2007, is the corporate body within the BCI numbering some 60 organisations including BAE Systems, BP International, BSi Management Systems, BT, Community Resilience, Continuity Shop, ContinuitySA, EADS, Garrison Continuity, Marsh, HBOS/Lloyds Banking Group, HP, Milton Keynes Council, Prudential, Royal Mail, SunGard, and the UK government’s Cabinet Office.

Contacting the Business Continuity Institute

Lee Glendon
Campaigns Manager
The Business Continuity Institute
Telephone: +44 118 947 8215
Email: lee.glendon@thebci.org
Internet: www.thebci.org

End of document.