Corporate Governance & the Financial Crisis

A response to the OECD public online consultation from the Business Continuity Institute

The Business Continuity Institute is pleased to respond to the consultation with respect to the questions on the Implementation of Risk Management.

This response was written by Lee Glendon and approved by Lyndon Bird FBCI, Technical Director at the Business Continuity Institute.

The Business Continuity Institute, 10-11 Southview Park, Marsack Street, Caversham, RG4 5AF, United Kingdom.
Telephone: +44 118 947 8215; Email: bci@thebci.org; Website: www.thebci.org

Implementation of Risk Management

Introduction

Have Non Executive Directors been dazzled by the false reassurance of risk models?

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 event[1]. Another issue indicated in the OECD report[2] is that Boards lacked a clear understanding of the changing risk profile of the businesses they manage.

So if the current approach to risk management has inherent weaknesses and is too complex as a corporate governance tool, is there an alternative approach? We believe that the Business Continuity Management (BCM) framework can provide answers to these questions and we have outlined our thoughts below and included a case study from a bank which applied the BCM framework to prepare itself for the collapse of a major counterparty, which eventually happened in September 2008.

What is the most important step a company can take if it wants to improve its risk management system?

The Business Continuity Institute recommends 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 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 from the impact of disruption and in the event of a disruption question the plans for responding to and recovering from it.

We would recommend this new focus on event impacts rather than risks. There are many risks but event impacts are generally limited to key processes and/or assets. Impacts can also be assessed objectively whereas risk assessments are highly subjective. A problem with governance at risk-level is that there is a high level of duplication. From a policy perspective it is easier to detail and review event impacts rather than risk.

An event impact can be felt on one or more of the following:

- Reputation
- Customers
- Suppliers
- Finance
- People
- ICT
- Facilities

[1] Global Risks 2009, A World Economic Forum Report, January 2009, page 11.
[2] Corporate Governance Lessons from the Financial Crisis, OECD 2009.

Working backwards it is clearly possible to develop an approach to deal with seven impacts rather than an extensive risk register with overlapping impacts. 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*.

It's also worth noting that the origins of an idea are important – 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. In traditional risk management, risk can be transferred or avoided, in reality this creates a false sense of security as the impact of not dealing with a significant disruption is still felt by the organisation and risk transfer cannot cover the loss of reputation and long term impact of not being seen as a well run business.

Nevertheless risk assessment is still necessary within an organisation however it needs to made in the context of preserving the value creating processes of an enterprise as identified in the Impact Policy and sit a little further downstream that its current position.

How shall the internal governance structure be designed to support active and effective implementation of risk-management throughout the company?

The key proposal from the Business Continuity Institute is for an Impact Policy to be developed and managed at Board level and be an integral part of a reformed corporate governance model.

In Figure 1 we have outlined an evolved framework from the BCI's Good Practice Guidelines for Business Continuity Management[3] which could be applied within a wider corporate governance model.

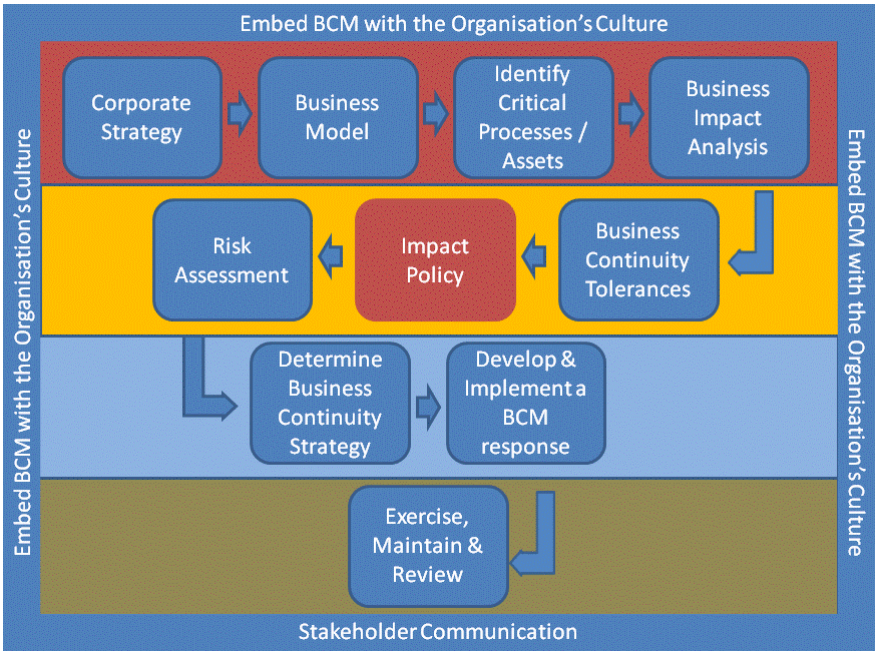

Figure 1: An Evolved Business Continuity Management Framework

In this model the Board will focus on corporate strategy development and understanding the business model as per today, however prior to any risk assessment activities the Board will identify and document critical processes and assets which underpin its ability to create value for its shareholders. The criticality of these processes and assets will vary from organisation to organisation and should not be defined at this level.

[3] BCI Good Practice Guidelines 2008 for BCM, embedded at the end of this document.

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.

From this stage 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.

Up to this point no one has been asked for any risk assessment, 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 maximising the "up-time of" or "access to" these processes and assets.

The Risk Assessment phase is now focused on any risk that has an impact on the above, arguably devoid of any arbitrary view on probability.

The next stages are to be conducted at the specialist operational level of the organisation and will look at determining the Business Continuity Strategy and developing and implementing the BCM response.

The final two stages do require direction and investment of time and resources from the Board. Our case study with Euroclear Bank shows there is no substitute for testing out an organisation's systems and plans but these can be expensive and time consuming, so top level support of regular testing of procedures to deal with major impact events is required.

The final stage effectively supports the whole framework and concerns the need to embed good practice throughout the organisation. The BCI recommends at least compliance with available standards in Business Continuity Management but in some case organisations may choose external certification to provide an independent view on 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.

Board (Audit) Committee – The Audit Committee should require regular exercises to test the organisation's commitment to the Impact Policy. We would advocate that at least one Non-Executive takes on responsibility for Business Continuity Management oversight.

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".

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.

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.

Conclusion

Whatever the causes of the current crisis, we feel that more complexity is not going to solve the problem. Complexity is the enemy of understanding. 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 critical assets, processes and vulnerabilities would appear to be a logical role for the Board and tenet of corporate governance. The development of an Impact Policy would provide a much clearer direction to the company's underlying businesses and be easier to manage from the Board.

About Business Continuity Management

Business Continuity Management (BCM) identifies potential threats to an organisation and the impacts to business operations that those threats if realised might cause. 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.

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 4,500 members in over 80 countries active in an estimated 3,000 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 Marsh, PwC, Aon, Prudential, HP, SunGard, BT and the UK's Cabinet Office.

Additional Documentation (embedded)

- The BCI's Good Practice Guidelines 2008 Section 1 and 2.


GPG2008V1 Section1.doc


GPG2008V1 Section2.doc

- The Euroclear bank case study.


Euroclear Bank case study.pdf

Contacting the Business Continuity Institute

For any questions, please contact the following person:

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

End of document.