May 2009

Financial Reporting Council
Review of the effectiveness of the Combined Code
Call for Evidence

Response from the Business Continuity Institute to Question 12, the role of the board in relation to risk management.

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 an OECD report[2] is that Boards lacked a clear understanding of the changing risk profile of the businesses they manage.

The Business Continuity Institute believes we should therefore resist demands for "more" risk management and consider what we are trying to achieve**.** Corporate Governance seeks to assign accountability and deliver transparency to stakeholders, risk management has failed to deliver here. This response outlines how the Business Continuity Management (BCM) methodology can provide a coherent response to some of the problems experienced.

The core problem has already been identified - risk issues have increasingly become too specialist for meaningful oversight by the whole board. 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.

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.

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. None of these impacts should be a surprise and People, ICT and Facilities 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*.

Threat identification, assessment and reporting are still necessary within an organisation. However it needs to made be within the context of preserving the value creating processes of an enterprise as identified in the Impact Policy and sit a little further downstream than its current position in the process.

The key proposal from the Business Continuity Institute is for an Impact Policy to be developed and managed at Board level and become 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.

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

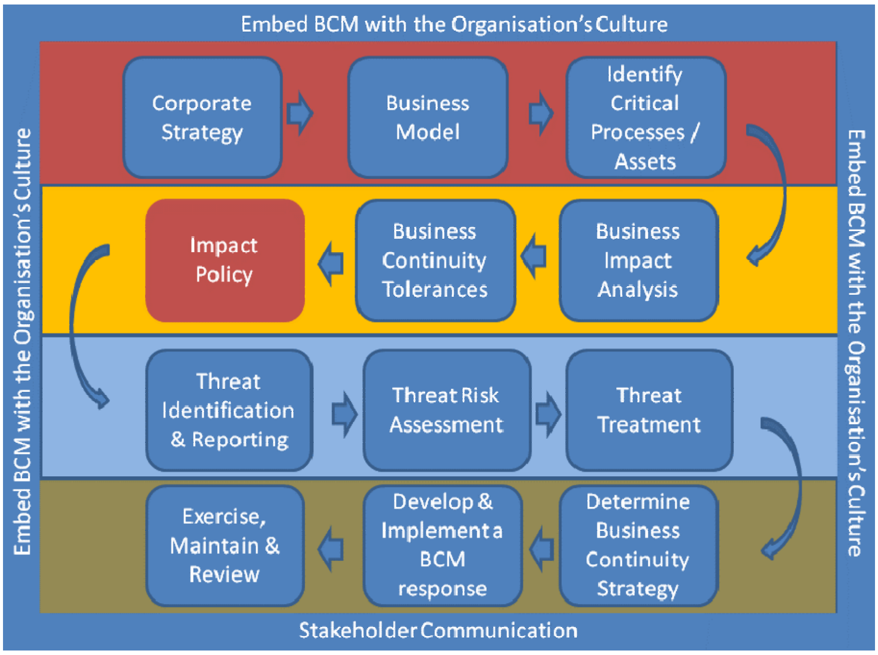
Embed BCM with the Organisation's Culture
Corporate Strategy
Business Model
Identify Critical Processes / Assets
Impact Policy
Business Continuity Tolerances
Business Impact Analysis
Threat Identification & Reporting
Threat Risk Assessment
Threat Treatment
Exercise, Maintain & Review
Develop & Implement a BCM response
Determine Business Continuity Strategy
Embed BCM with the Organisation's Culture
Embed BCM with the Organisation's Culture
Stakeholder Communication

Figure 1: An Evolved Business Continuity Management Framework

In the next step the question is asked what would be the impact on the business if these processes failed or an asset were 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.

[3] The BCI's Good Practice Guidelines (GPG) 2008 for BCM are available to download free of charge from the website - www.thebci.org

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.

Up to this point no one has been asked for any threat 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 Threat Assessment phase is now focused on any threat 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. There is no substitute for testing out an organisation's systems and 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. Ensuring that plans and exercises reflect organisational development is vital such as following mergers, acquisitions and divestitures.

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.

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] *Stress testing* and related scenario-analysis are important business continuity management tools.

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 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.

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 response 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.

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 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.

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 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, PwC, 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.