

“Although there is no such thing as the right time for a crisis, any time is a good time for developing even a simple approach to BCM”

A RISK-BASED APPROACH TO BCM

Julia Graham examines the relationship between risk management and business continuity management and highlights the unity which enterprise-wide risk management may bring

The way that all organisations monitor and manage risk from day to day is becoming an ever higher business and board agenda item. No business, whether a high street store, a financial institution or a retail manufacturer can escape from the impact of the changing severity in risk profiles resulting from multiple threats, including global warming, global terrorism, global crime and now the global credit crunch.

What keeps your CEO awake at night?

- Financial volatility
- Regulation
- Reputation
- Catastrophe
- Energy availability
- Supply chain

Risk Manager Survey – Business Insurance Europe: 2008

According to American risk management guru Felix Klotman, risk management strategies should address three separate goals:

1. build and maintain the confidence of stakeholder groups;
2. encourage opportunism; and
3. teach organisations how to cope with uncertainty and doubt.

Specifically, business continuity management has a leading role to play in the management of risk and in the management of uncertainty and doubt. More generally, where does BCM fit into this global risk scenario? The answer is, “everywhere”.

There has been a growing realisation that businesses need to manage all risks, tangible and intangible, and as a key control mechanism BCM must rise to the challenge. The silos of risk management are being drawn closer together into an integrated enterprise risk management (ERM) framework. Whether the drivers for

change are internal to an organisation or external through governance, regulatory or legislative pressures, risk management and business continuity management have come of age as united disciplines.

Complementary disciplines

BCM must dovetail into every aspect an organisation might need to risk manage, as an enterprise-wide control mechanism. This said, it is only after an organisation has analysed its business and understood its risks, that it can design and implement an effective business continuity response.

As risk management can lead to a better understanding of an organisation and its business, so business continuity can provide the strategic and operational framework to review the way an organisation provides its products and services – while improving resilience to disruption, interruption or loss.

Basel II defines operational risk as, “the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events”. Risk management, and notably operational risk management, and BCM are complementary disciplines.

The focus of business continuity is on prevention, about understanding what might be at risk, about making judgements, about criticality, and then about developing strategies and solutions to reduce the severity of the risk, and be able to respond to the risk with robust plans if it does occur.

The policies, procedures and structures in most organisations are designed for normal operations and in general are unsuitable for dealing with sudden and unexpected events. Although there is no such thing as the right time for a crisis, any time is a good time for developing even a simple approach to BCM. But such an approach will only have a chance of succeeding if it has senior management buy-in and has been developed following a systematic management process in tune with an organisation’s culture, complexity, internal and external needs, and

is maintained and exercised.

The focus of risk management is about managing uncertainty, about systematically and proportionately addressing the risks around the organisation’s activities whilst supporting continuous improvement.

As with business continuity, risk management will only be effective if it has the support of senior management and follows a systematic management approach. Consequently, there is a great deal of commonality between the disciplines. Both disciplines:

- are dependent on an understanding of the context within which the organisation operates;
- must recognise and respect the culture of the organisation;
- reflect the nature, scale and complexity of the organisation; and
- use programme management and a framework at the centre of the lifecycle or process.

These similarities are illustrated in Figures 1 and 2, which are taken respectively from BS25999 (Code of practice for business continuity management) and BS31100 (draft code of practice for risk management).

Figure 1 – The Business Continuity Management Lifecycle (BS25999)

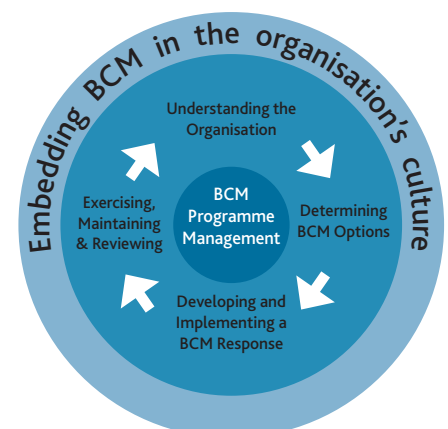
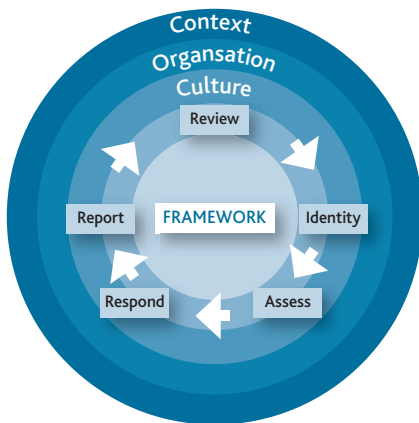


Figure 2 – The Risk Management Process (BS31100 – Draft)



Who takes responsibility?

There is still a considerable debate as to whether risk and business continuity management should be closely aligned and form part of the same departmental function. There is no right answer to this question. Whether these roles should sit together is a matter for each organisation to consider and will be dependent upon the framework and approach taken for managing governance and risk.

In larger organisations, a range of dedicated risk and business continuity roles may exist which could be positioned in a range of departments. For example, those charged with leading the development and implementation of IT-related business continuity may best sit within the IT function, while others charged with non-IT-related responsibilities may sit more appropriately elsewhere, including risk management and as part of this, operational risk management. But caution should be exercised in creating roles and teams which are positioned in such a way that it inhibits their integration with the business, and promotes isolation from the skills and resource they require from others to effectively deliver their responsibilities.

This said, a board more often recognises the strategic importance of risk management and considers this as a board agenda topic – whereas BCM is more often relegated to the second division of issues for the ‘technical people’ in IT, facilities or the like to consider and manage. Managing the disciplines in an integrated way may help to open the boardroom door to the business continuity professional.

Whatever the approach, a factor for success will be the production and adherence to clear and unambiguous job profiles. Job profiles will be driven by an organisation’s approach to profile design, the objectives and scope of roles and responsibilities, the source and level of authority, and the skills and experience required to deliver the role effectively.

Business Continuity Institute (BCI) structure for the certification of business continuity practitioners

- BCM policy and programme management
- Understanding the organisation
- Determining business continuity strategies
- Developing a business continuity response
- Exercising, maintenance and review
- Embedding business continuity within the organisation’s culture

www.thebci.org

However, profiles should also recognise that while many of the skills required of the risk manager and business continuity manager are shared, others are not – competence in exercising, rehearsal and response are more often in the domain of the business continuity manager.

Fit for the job

Put simply, to achieve the maximum improvement in the position and focus on BCM, recognition by an organisation of the importance of a role designed to help build resilience, and to respond following an incident, is critical.

An organisation that provides clearly defined roles and responsibilities with effective performance management will have a firm foundation for extending core management practices and behaviours into those associated with business continuity management.

The Institute of Risk Management (IRM) Certificate syllabus sections

- Introduction to risk management
- Risk strategy
- Risk assessment
- Risk and organisations
- Risk response
- Risk assurance and reporting

www.theirm.org/Qualifications/certStructure.html

BS25999 addresses how an organisation might manage business continuity but states “individuals tasked with implementing and maintaining the business continuity programme may reside in many areas of an organisation depending on its size, scale and complexity. It is essential, however, that a person with appropriate authority (e.g. owner, board director or elected representative) has overall responsibility for BCM and is directly accountable for ensuring the continued success of this capability”. (BS25999 – 2006)

(There is less ‘navel gazing’ about the position of risk management within the

organisation in BS31100 (draft) indicating perhaps a greater degree of assurance and confidence that with the right approach this will reach the board’s attention).

Enterprise Risk Management

A unifying force is the development of Enterprise Risk Management (ERM) which is broadening the past risk management focus.

There are three key elements in a successful ERM lifespan

- Strategy
- Resources
- Culture

Aon Enterprise Risk Management – the full picture 2008

There remain significant differences between definitions of what is meant by ERM, models or frameworks for describing risk management activities, and how far along the route towards ERM implementation organisations have travelled. Definitions generally should however embrace process, outputs and impacts.

Common risk framework elements identified in a report by AIRMIC, the association of insurance and risk managers (Research into the Benefits of Enterprise Risk Management – undertaken by DNV for AIRMIC – June 2008) identify with the Aon research and include:

- Purpose
- Commitment
- Capability
- Learning

What seems apparent is that ERM delivers a number of benefits including better decision-making, delivery of projects and targets, and improved governance – all key for the delivery of a successful strategy for risk management and business continuity management.

Not surprisingly, research confirms that ERM is still a rapidly developing discipline and that risk (and business continuity) professionals continue to learn from experience and contribute to developing best practice. The journey continues...

JULIA GRAHAM FBCI

Julia Graham is Chief Risk Officer at DLA Piper UK LLP

www.dlapiper.com