

BUSINESS CONTINUITY MANAGEMENT

“Do you measure up?” asks Michael Gallagher

Business Continuity Management (BCM) has moved rapidly up the boardroom agenda. Just a few years ago it scarcely featured on the agenda at all. September 11 and other incidents and disasters - both natural and man-made - have meant that it has assumed a much higher profile. It should be a real concern of the board and of the audit committee.

Regulatory and corporate governance requirements have insisted that both board members and executive management take BCM seriously. Insurance has also become a key driver. Many insurers are now insisting that organisations must demonstrate that they have reasonable risk reduction measures and a working business continuity programme in place. Previously insurance companies might have offered a discount on the premium if such a scenario existed. Now they may not even be prepared to provide cover unless they are satisfied that there is a strategy in place, that plans have been documented, and they are provided with evidence that these plans have been tested or exercised.

This article defines BCM and it also attempts to provide a quick means of determining how your organisation measures up - how well has it prepared itself to ensure that it continues in business in the aftermath of a serious incident?

Gartner estimates that two out of five enterprises that experience a disaster will go out of business within five years. Enterprises can improve these odds - but only if they take the necessary measures before and after the disaster.

Aftermath: Disaster Recovery, Gartner, September 2001

What is BCM?

To some extent BCM grew out of IT Disaster Recovery Planning. While IT disaster recovery plans are still very important, BCM is now regarded as being concerned with every aspect of an organisation's operation - not just IT. It is not just about recovering from a disaster such as one caused by fire or flood or the failure of computer systems. It can also be about the collapse of a key supplier or customer, an industrial dispute which halts critical supplies, loss of a key executive, an infectious disease epidemic, anthrax-type scares, fraud, unethical operations, environmental pollution and reputation management.

The Business Continuity Institute (BCI) defines BCM as "the act of anticipating incidents which will affect mission-critical functions and processes for the organisation and ensuring that it responds in a planned and rehearsed manner".

The BCI definition emphasises three key elements -

- "It is the act of anticipating incidents"

The organisation must examine the risks and threats to which it is exposed and consider how best to deal with them should an incident occur. The choice of the word incident rather than disaster is important.

- "Which affect mission critical functions and processes"

BCM is not about plans and procedures for the everyday

things that go wrong. It is concerned with significant incidents which have a considerable impact on the core activities of the organisation. It is far too easy to divert effort into documenting procedures for the failure of day-to-day operational processes. While these procedures must exist, BCM must emphasise the big picture.

- "Ensuring that it responds to any incident in a planned and rehearsed manner"

This element of the definition encompasses the planning, the meaningful involvement of appropriate personnel, acceptance and ownership of the plan, and thorough testing all of which are essential prerequisites of an appropriate response.

Where do you stand?

The set of questions opposite provides an attempt to allow you to establish where your organisation is in relation to BCM. Score each section in the range 0 to 5 where 0 indicates that the topic(s) has not been addressed at all to 5 where you are satisfied that you have reached the point where you are happy with the situation in relation to the main issues raised.

How did you measure up?	
It is not easy to construct a checklist which applies equally to all types of organisations. Clearly some issues are more significant in particular industries. Nevertheless, the following is a general guide to the significance of your score.	
Over 80	It is likely that there is an effective BCM programme in place.
65 - 80	If regulatory BCM requirements apply to your organisation it is unlikely that they are being met.
50 - 65	There is room for improvement. You are probably not complying with good governance requirements.
Less than 50	Considerable work to be done to achieve a satisfactory state. Directors should be concerned and should be asking serious questions.

*Michael GALLAGHER is a member of the Business Continuity Institute and vice-chair of the Irish branch of the Emergency Planning Society. His book, Business Continuity Management - How to Protect your Company from Danger, is published by Financial Times / Prentice Hall in their Executive Briefing series (www.briefingzone.com)
E-mail gallagml@iol.ie*

BCM Self Assessment Questionnaire

Score 0-5

1	Is there an active BCM programme in place in your organisation? Is BCM a comprehensive activity, which is closely linked to risk management, IT security, physical security, insurance, internal audit, etc?	
2	Is there a person appointed with overall responsibility and authority for managing the programme. Is there a sponsor at board level? Does a Planning / Steering committee, or a BCM Working Group exist? Is this group representative of all main functions / departments?	
3	Has a risk management / BCM culture been established? Are both senior and middle management aware of the issues? Is BCM regarded as part of a manager's job specification and does it rank as a Key Performance Indicator in the annual performance evaluation and appraisal process?	
4	Is business continuity something which must be taken into consideration in preparing proposals for new projects or in seeking approval for capital expenditure? Does the approval process insist on this?	
5	Has a risk analysis or business impact analysis been done and has management endorsed the priorities which that process has defined? Have controls and safeguards been identified and implemented to minimise loss?	
6	Are regular reports on business continuity status, targets and achievements made to executive management and to the board?	
7	Are there documented business continuity plans? Have key executives got a copy of the plan(s) at a location, at home for example, where it would be quickly accessible in the event of an incident? Are the plans in a format which is usable in the event of a crisis?	
8	Is there an Emergency / Crises Management Team? Are key executives aware of the plan and of their roles in a crisis? Has a location for a crisis command and control centre been identified? Are arrangements in place to move to alternative sites if required?	
9	Are business continuity plans exercised regularly - has an exercise taken place within the past six months? Are these exercises realistic? Are the results of such exercises / tests documented and used to influence the work programme?	
10	Does the plan deal with how to handle the media? Are managers aware of the procedures to be followed for both internal and external communications?	
11	Does the plan deal with people issues - relocation arrangements, communication with next of kin and provision for trauma counselling where necessary?	
12	Are arrangements for IT resilience and contingency adequate? Do these include built-in redundancy, multiple nodes, clustering, mirroring, multiple locations, hot-sites, etc. as appropriate?	
13	Have user departments been involved in creating the IT Disaster Recovery Plan and have they been involved in testing the plan? Are user department processes taken into account in plan testing, or is testing confined to recovery of computer hardware and software?	
14	Are backup and recovery procedures reviewed and tested regularly? Are backup power arrangements in place and tested regularly?	
15	Are the backup and resilience features of the voice and data communications infrastructure adequate? If these facilities are critical to the business, have the alternative arrangements been tested within the past six months?	
16	Are documented IT security policies and procedures in place? Are all computer users fully aware of e-mail and internet usage policies?	
17	Is computer anti-virus software kept up-to-date? Are computer error and exception logs adequately monitored? Is there an IT Incident Response Plan and are all relevant personnel familiar with it?	
18	Has the role of, and relationship with, public authorities been considered? Is there an awareness concerning risks of environmental pollution? Have health and safety issues been considered? Has a good working relationship been established with the local emergency services?	
19	Do contracts with key suppliers require that these organisations have a BCP? Is BCM included in the contracts for all outsourced business functions? Have these plans been reviewed by your organisation within the past year? Have tests / exercises been observed or reviewed?	
20	Are business continuity plans updated regularly? Are contact details up to date and do plans reflect the current organisation structure and responsibilities? Have the plans and processes been audited / appraised by an independent internal source or by external experts?	
		TOTAL SCORE