

# BUSINESS AS USUAL

Business continuity management programmes should be risk-based and consider all potential threats to the business, says **Gareth Book**

Increasing pressure from existing and potential customers, corporate governance requirements and insurers, is forcing organisations to look more closely at business continuity management (BCM) as part of their overall risk management strategy. However, although there have been significant increases in concern about the range of potential threats facing businesses, business continuity plans (BCPs) still tend to focus on a relatively small number of well-established types of disruption, ignoring potentially significant threats.

In its 2004 Annual Business Continuity Survey, the Chartered Management Institute identified only four kinds of disruption – loss of IT, loss of telecommunications, loss of site, and fire – that were covered by a significant majority of BCPs. Although these clearly represent key threats to businesses, it is worrying that the increasing number of organisations aware of a greater range of threats are not reflecting this in their business continuity planning.

## Risk-based approach

It is unrealistic to expect a BCP to address every threat facing a business, no matter how unlikely it is or how trivial the impact. If it did, it would be unusable. It is therefore critical that businesses utilise a risk-based approach, to ensure that BCPs address the threats which present the greatest risk to the business, not only the worst-case impact, which is often the case. To do this, businesses must systematically identify all internal and external threats, assess the risks associated with them and assure themselves that business continuity risks are being effectively managed through a formal risk management process.

Figure 1 outlines five stages in implementing a risk-based business continuity management process.

### STAGE 1 – UNDERSTAND THE BUSINESS AND IDENTIFY AND ASSESS THE BUSINESS CONTINUITY RISKS

The first stage is to undertake a business continuity risk identification and assessment workshop. Central to this is identifying the critical business processes, the impact on the business from failures of these processes and the current controls in place to prevent or mitigate such failures.

The workshop should consider all potential threats to the business, not only those with the worst-case impact. It is therefore important to involve personnel from all areas of the business to ensure all threats are identified and the associated risks are accurately evaluated.

The risks identified should be assessed and prioritised in the workshop using a risk matrix (figure 2) calibrated specifically for the operations being assessed, by taking into account the recovery time objectives for the business.

In setting the business impact criteria, you need to consider the nature of the operations (real-time, just-in-time, lean enterprise), the level of resilience in the operations (spare capacity, spare equipment) and the relationships with key customers and suppliers.

The output from this stage should be a comprehensive business risk register, identifying and priori-

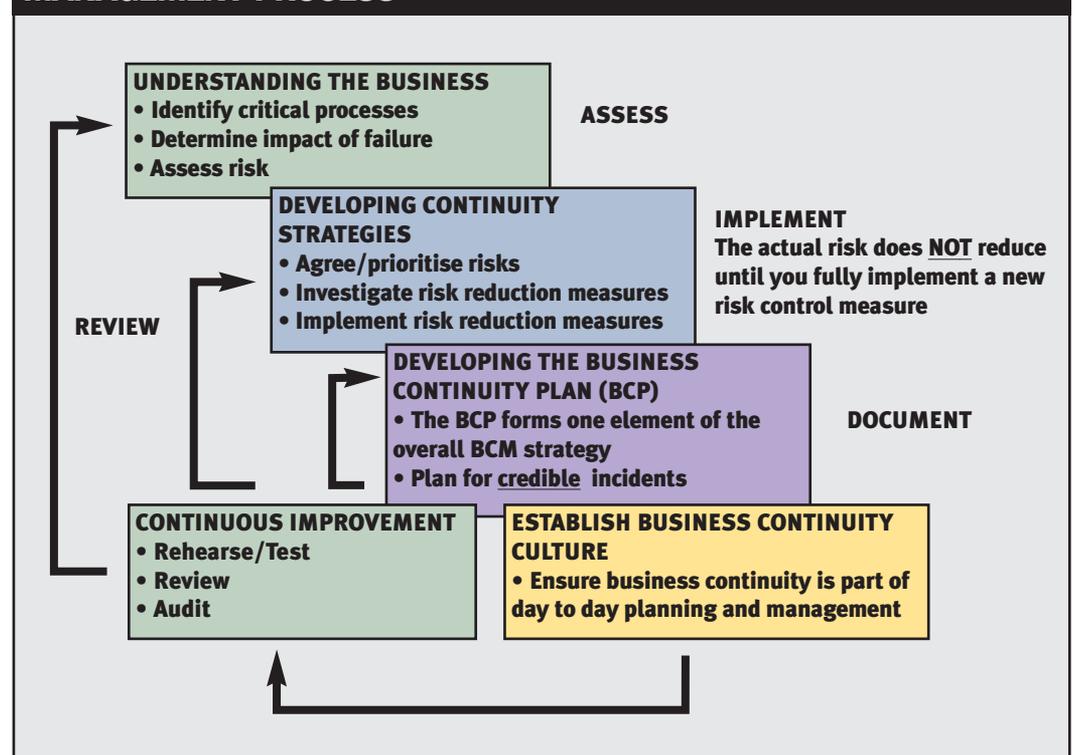
tising the key risks facing the business together with a remedial action plan to address any perceived weakness in the current management arrangements.

### STAGE 2 - DEVELOPING BUSINESS CONTINUITY MANAGEMENT STRATEGIES

The next stage is to identify strategies to reduce the risk for the key scenarios identified in the workshop. BCM strategies should be identified and implemented to reduce the risk as low as is reasonably practicable before developing detailed BCPs. In our experience, prevention is generally much more cost effective than dealing with emergencies.

The suitability of alternative strategies should be assessed against the output of the risk assessment and, if necessary, cost-benefit analysis of them may be performed. Following implementation, the 'base case' risk score assigned in the workshop should be

**FIGURE 1 – FIVE STAGES OF A RISK-BASED BUSINESS CONTINUITY MANAGEMENT PROCESS**



# It is unrealistic to expect a plan to address every threat

updated to indicate the 'residual' risk, remembering that the actual risk does not reduce until you fully implement a new risk control measure.

### STAGE 3 – DEVELOPING THE CONTINUITY PLAN

It is essential that the BCP reflects the risk profile for the business and not simply a generic list of threats. There is little value in spending time, effort and money developing BCPs for threats which are either not credible or have a sufficiently low impact that they can be managed through normal business processes. BCPs should therefore focus on the credible high-risk scenarios identified in the workshops.

Similarly, the selection of the BCM team should also reflect the risk profile for the business. It may help to think of the team in terms of a squad, which consists of a small number of key individuals who are always involved in BCP incidents, and a larger number who are co-opted to the team depending on the nature of the incident. In this way the most appropriate team is selected for the incident.

For example, an IT manager is unlikely to be involved in responding to an environmental incident which results in a shutdown of a manufacturing plant. Conversely, an environmental health and safety manager should not need to be involved in responding to an IT system crash. In both cases, however, there is a potentially significant financial impact (fines, lost production and possible lost sales) so the finance director or someone holding a similar position should be involved. Of course, the exact composition of the BCM team will depend on the nature and size of the business.

### STAGE 4 – ESTABLISH BUSINESS CONTINUITY CULTURE

It is important to recognise that documenting the BCP is only one part of the overall BCM process. Its success is thereafter dependent upon embedding a business continuity culture throughout the business. This is best achieved by involving all stakeholders in the BCM process, providing training to those directly involved in the execution of the plan, including rehearsing and testing the BCP, and raising awareness of BCM to ensure its company-wide adoption.

In our experience, including the roles and responsibilities of BCM team members within their job descriptions can be a very effective way of embedding a business continuity culture in an organisation. This ensures that business continuity arrangements remain current even when people move positions.

### STAGE 5 – CONTINUOUS IMPROVEMENT

BCM is a continuous process; it does not end following documentation of a BCP or completion of a risk assessment workshop. In addition to regular rehearsing, testing and auditing of the BCP, you should regularly review the risk register to check that the risks are being effectively managed and ensure that emerging risks to the business are identified and assessed.

Benchmarking using tools such as the BCI PAS 56 Audit Workbook or self-assessment questionnaires allows organisations to determine the maturity of their BCM systems and also provides a useful mechanism to drive continuous improvement in these systems.

## Summary

In summary, a risk-based approach to BCM focuses resources on the threats which present the greatest risk to the business.

By using a risk-based approach, businesses will be better prepared to prevent and mitigate business interruption losses more efficiently and clearly demonstrate to all stakeholders (regulators, investors, insurers, customers and employees) that business continuity risks are effectively managed through a formal process.

Gareth Book is a principal consultant at Risktec Solutions, Tel: 01925 431010

## PAS 56

The British Standards Guide to Business Continuity Management (BCM), PAS 56, is an important step in driving businesses to adopt a risk-based approach to developing BCPs. And it is highly likely that insurers and customers will start to ask businesses whether they are PAS 56-compliant. PAS 56 was published in 2003 by the British Standards Institution and will be the UK's first publicly recognised standard for business continuity management. In August, Marsh issued guidance on the new standard and its recommendations.

PAS 56 makes a number of initial recommendations about what is needed for BCM to be effective in an organisation. They include that BCM should:

- be a business-as-usual process driven from the top of the organisation
- be fully endorsed and actively promoted by the board
- have a member of the board or executive committee assigned overall accountability for the effectiveness of the organisation's BCM competence and capability
- be managed at operational and organisational levels.

The standard also identifies that BCM should directly support the business strategy and be designed to protect and optimise product and service availability.

The core part of PAS 56 is built around the 'BCM life-cycle', a continuous cyclical process intended to underpin the business continuity activity of any organisation. Through every stage of this cycle, the standard outlines a general definition for each of its component parts, the purpose of that exercise and the outcomes an organisation should expect from that stage of the process.

Although PAS 56 is not currently mandatory, Marsh says that it is considered to be the single recognised benchmark in the UK against which business continuity best practice can be evaluated. 'Those organisations choosing to ensure that their business continuity meets its recommendations will create competitive advantage against other organisations in their sector who do not.'

The BSI reports a high take-up from companies. Institutional stakeholders, such as investors and insurers, are already specifying that they will look for their clients to be able to demonstrate that their business continuity management meets the criteria set out by PAS 56. Early evidence from the insurance market suggests that companies that can demonstrate this are likely to receive preferential terms.

(Marsh Adviser PAS56 Guide to Business Continuity Management August 2004)

**FIGURE 2 – EXAMPLE OF A BUSINESS CONTINUITY RISK ASSESSMENT MATRIX**

Severity	Business Impact  Impact on delivery of product to customer	Increasing Likelihood				
		A	B	C	D	E
		Never heard of in the industry	Has occurred in company	Has occurred in company	Happens several times per year in company	Happens several times per year at site
0	None					
1	Trivial					
2	Impact < 12 hours					
3	12 hours < Impact < 48 hours					
4	48 hours < Impact < 1 week					
5	Impact > 1 week					

MANAGE FOR CONTINUOUS IMPROVEMENT

DEVELOP RISK REDUCTION MEASURES

INTOLERABLE