Risk Management Guidelines

[Business Continuity Management]

Understanding Risk

We live in an unpredictable world. No matter how effectively a business protects itself through insurance, there are some risks that cannot be anticipated, nor insured. Appropriate insurance can provide monetary protection in case of events such as fire, flood, denial of access or acts of terrorism. Typically cover relates to the shortfall in gross profit for a specified period following the damage event. However, insurance can never provide total security against the long-term or permanent loss of

- customers
- brand value
- share price
- markets
- quality
- key employees

The only effective protection against serious disruption of your business is Business Continuity Management

The following are designed to help you to alleviate the effects of an incident and to develop a recovery plan tailored to the needs of your organisation.

Business Continuity Management

Business Continuity Management (BCM) is about having resilience to business interruption and 'just-in-case' recovery procedures for business-critical processes.

These recovery procedures take the form of a Business Continuity Plan (BCP) that includes the key actions, personnel, contact information and services needed to manage the incident and the recovery process. The breadth and depth of planning will depend upon the size, nature and complexity of your organisation.

Getting started

You should start by asking yourself these questions:

- How complex is our business?

  The nature of the business and its operations will be a major factor in considering recovery strategies.

- What size is our business?

  This has a bearing on how many people you would need to involve both in the planning and the initial recovery process and how you organise into teams.

- Which processes are business-critical?

  Prior knowledge about which parts of your business must be given recovery priority is fundamentally important.

- What resources will be required?

  You will need to make an early assessment of the likely costs of planning and recovery. You will then need to budget accordingly.

- Who should be involved?

  You will need to involve people with the right skills and experience.

Risk Management Guidelines

Business Impact Analysis

In the aftermath of a disaster there will be competing requirements for recovery. Business impact analysis (BIA) provides the necessary focus for prioritised recovery of business-critical processes. The purpose of BIA is to:

- identify and evaluate business-critical processes;
- prioritise reinstatement or replacement needs;
- identify resource requirements to achieve this.

The easiest way to address BIA is to list all your processes and decide (*yes* or *no*) whether you consider them to be business-critical. Bear in mind that, whilst some processes may not be business-critical all the time, you need to be planning recovery from a worst case and timing of an event or set of circumstances.

Where the answer is *yes*,

- Apply a scale (say 1-3 with 1 being highest priority), to recovery priorities.
- Decide what facilities and resources would be required to achieve these recovery priorities.
- Give realistic consideration to how quickly the resources could be replaced or alternatives made available.
- Use this information as the basis for developing your recovery strategies.

Risk Assessment

Risk assessment is about understanding the business interruption risks to which your organisation is exposed, the likelihood of occurrence and the probable level of impact.

The benefit of carrying out a risk assessment is the assurance that appropriate loss prevention and damage limitation arrangements are in place. The benefit of carrying out the BIA, as well as the risk assessment, is that it enables you to focus attention on activities, processes and resources that have been identified as 'business-critical'.

Risk assessment is a required procedure for health and safety in the workplace and the same approach should be used for BCM. The purpose is to:

- Identify and measure the risks (fire, flood etc.) and threats (loss of power, communications etc.) to your business;
- Review the controls in place to reduce risks and threats;
- Reduce the risks and threats, where necessary, by implementing further controls;
- Assess the impact on your operations should a loss happen.

The main areas that should be addressed are 'hardware' – the physical arrangements in place – for example fire detection and suppression devices and security installations, and 'software' – for example the human element, operating procedures, training and working practices.

Risk Management Guidelines

Risk assessment is accomplished by a combination of physical inspection and by review of the procedures and practices in place. The outcome of the process will result in a better understanding of your business interruption exposures and resilience and will provide you with the opportunity to make appropriate improvements to your risk control measures and programmes.

Listed below are the major headings for evaluation with examples of the issues to be investigated:

The organisation

What are your key activities and processes, how 'immediate' would be the effect of interruption?

Premises

Are they specialised or 'standard'; what alternatives are available; does location matter; how long to re-build; is there likely to be planning opposition, special conditions, difficulties with site access?

Key personnel

Do you have key teams or individuals; is there loyalty and flexibility, are they readily replaceable; are they deputised; do they have unique knowledge or contacts?

Customer base

Are you a 'just-in-time' business; how fierce is competition; what is the level of customer loyalty; are there seasonal/periodic peaks to your business?

Utilities

What is your reliance upon electricity, gas, water; what is the resilience of supply; what are your fallback arrangements?

Plant & equipment

Are there production or process 'bottlenecks'; are there long lead times for key items; what is the history of breakdown; are strategic spares kept; where are these located?

Product

What are the lowest quantities and highest demand levels for raw materials, components, finished goods and consumables; how long to replace; is direct supply to customers possible?

Technology

How important is IT and telecommunications; is there adequate physical protection; how long for system hardware and software replacement; what service level is contractually provided; do you have stand-by power?

Data

Do you have vital paper based or electronic data; is confidentiality, integrity and availability adequate; are back-up arrangements for data and software appropriate?

Suppliers and sub-contractors

Are these vital to your operations; what is their resilience to supply interruption; are there alternatives?

Risk Management Guidelines

The Planning Phase

Developing the BCP

The prime requirement is to document or otherwise record the BCP to ensure its availability in the event of disaster. The plan should include:

- brief overview of objectives and strategy;
- team membership;
- roles, responsibilities and procedures;
- supporting database information.

Objectives & Strategy

The BIA process provides the base-line information on which to set the objectives and build the strategy that should identify recovery requirements and timeframes and alternative strategies for recovery. Examples of possible strategies include contracted assistance, alternative premises, alternative suppliers, direct supply and standby facilities.

Teams

Large organisations will require separate teams to plan and manage recovery; these may include:

Crisis Management Team

Emergency Response Team

Facilities Recovery Team

Technology Recovery Team

Business Recovery Team(s).

Smaller businesses may require fewer teams and very small organisations may require only a single team. Consider, however, the potential for trauma and stress and the workload that is likely to fall upon key individuals in the event of a major incident. Typical roles and responsibilities are set out below:

Crisis Management Team

Plan invocation, command and control; media relations; content of internal and external communications.

Emergency Response Team

Evacuation and employee and public safety; damage evaluation; post-incident security; emergency services liaison.

Facilities & Technology Recovery Team(s)

Provision of accommodation, furniture, plant, equipment, consumables, systems and data recovery

Business Recovery Teams

Recovery of business-critical processes, as pre-established.

These roles and responsibilities must be clearly defined but be sufficiently flexible to respond to unanticipated incidents and circumstances. There should be deputies to cover for absences.

Risk Management Guidelines

Invocation & Communication

Pre-define circumstances for plan invocation; give particular consideration to business-closed periods. Pre-define responsibilities within the plan. Use a 'cascade' or communication chain system when dealing with a large number of people.

It is essential that controlled communication be made with all potentially interested parties, as soon as possible. The BCP should include contact details and responsibility for ensuring that communication takes place and it is the right message. Those with whom early contact is essential are likely to include management and recovery teams, employees, shareholders, business partners, insurers, suppliers, customers, media, public authorities and sources of assistance. These may include disaster recovery service suppliers, building contractors, facilities and equipment suppliers, emergency glaziers and plumbers and utilities companies.

Awareness & Training

Training is the essential basis for assuring the ability of teams to respond effectively to a disaster. Initial training should address the need for, and the practical application of, BCM. Training will also arise as part of the plan preparation process where it will occur as part of checking the assumptions underpinning the strategy and validating the viability of the plan procedures and resources.

This element of planning and training is best achieved by the use of informal 'talks-through' of the procedures, adjusting and revising as required.

Ongoing training should be incorporated via the Review & Maintenance regime that should be part of ensuring continuing applicability of the plan and knowledge of those who have BCM responsibilities.

Security & Availability

The BCP needs to be available, no matter what the circumstances. The size of your organisation will dictate how many other people will need a copy of all or part of the BCP but, the more copies in circulation, the more complex it will be to maintain. Ideally, a full copy should be kept offsite, secured and readily available at all times and in all circumstances.

Record Keeping

Regardless of the circumstances of BCP invocation, it is imperative to keep written records. Benefits include the ability to carry out 'post-event' checks on the efficacy of the BCP, to capture details of expenditure, to control expenditure and to validate insurance claims. Each team should record all pertinent actions, resources used and expenditure.

Risk Management Guidelines

The Post Planning Phase

Exercising the BCP

Create a programme of periodic exercises, each designed to try out one or two components of your plan. (The invocation procedures are an important example).

Certain elements of Business Continuity Plans lend themselves more readily to physical testing, for example, IT recovery plans that are based upon a contractual response provide just such opportunities. 'Desk-top' exercises using pre-prepared loss scenarios should be used to exercise the integration of the full plan. As with all training and exercising, opportunity should be used to up-date, amend or add to the BCP, as necessary.

Review & Up-date Arrangements

BCM is a continuous process. As your business and its processes change, your BCP must reflect these changes and your teams must be able to respond positively. The BCP should include appropriate maintenance arrangements. The recovery strategy, procedures and supporting database should be reviewed at least annually. For most organisations, there will be need for more frequent reviews, particularly where there are changes of process, product, personnel etc.

In essence, the arrangements put in place should allocate clear responsibilities for review and up-date of risk exposures and controls, recovery priorities, strategy, recovery procedures, supporting data, training (including personnel changes) and BCP exercise and testing.

Your Business Continuity Plan could mean the difference between survival and failure.

However, it will only be as useful as the last time it was reviewed and up-dated.

For further information on this or any other related Risk Management topic please contact the Risk Control Unit in RSA Insurance Ireland Limited at 01 – 290 1123.