BUSINESS CONTINUITY INSTITUTE

GOOD PRACTICE GUIDELINES

2007

A Management Guide to Implementing
Global Good Practice in
Business Continuity Management

CHAPTER 3

ABOUT THE GUIDE

Introduction

The BCI published its first Good Practice Guidelines in 2002. This played a significant part in the development of the British Standards Institution's (BSI) Publicly Available Specification for Business Continuity Management (PAS 56). GPG05 was issued followed by an extensive rewrite in to take into account the latest thinking in BCM internationally and to recognise increasing maturity in BCM practice across all sectors, public and private.

This new guide to implementation of Business Continuity Management (GPG07) has been prepared to support the launch of BS 25999-1 A Code of Practice for Business Continuity Management by the British Standards Institution. It can be viewed as implementation guide to BS25999 and as a definitive text for those wishing to understand BCM principles and practices in a more comprehensive manner.

However as a global institute, The BCI needs to reflect good practice across the world. BS25999 offers a comprehensive view of the subject but there are other standards in place with which many BCI professional members need to understand. As such the GPG07 is also designed to cover the main requirements of NFPA1600 (US and Canada) HB221 (Australia), APS 232 (Australia) and FSA (UK).

In no cases, however, must the GPG be seen as a replacement for those standards or as a guarantee of compliance with those standards.

Format of Guide

The Guide has been prepared in 6 chapters, which are in line with the earlier versions of the Guide and also with BS25999 nomenclature.

Chapter 1 consists of the introductory information plus **BCM Programme Management**.

Chapter 2 is **Understanding The Organisation**

Chapter 3 is **DETERMINING BCM STRATEGY**

Chapter 4 is **Developing and Implementing BCM Response**

Chapter 5 is **Exercising, Maintaining & Reviewing BCM arrangements**

Chapter 6 is **Embedding BCM in the Organisation's Culture**

At the end of each chapter there is a summary of key learning outcomes that will support future use of the BCI Benchmarking tool, BCI E-Learning and BCI Entrance Examinations.

The view presented in these Guidelines attempts to provide the core discipline of Business Continuity Management while recognising that individual practitioners are often required, by common sense or direction, to extend their role because of the situation in the organisation they work for.

Before referencing this Chapter of the Guide, you are advised to read Chapter 1, which explains in more detail how the guide works and how to use it most effectively.

About Chapter 3 – Determining Business Continuity Strategy

Business Continuity Management is an holistic management process that identifies potential impacts that threaten an organisation and provides a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.

Determining Business Continuity Strategy is a key element of good Business Continuity Management. It seeks to build on the detailed analysis in the Understanding The Organisation stage in order to choose appropriate continuity strategies that meet the objectives defined in the BIA. It must support the organisation's objectives, obligations and statutory duties in a cost effective manner.

Chapter 3 – Determining Business Continuity Strategy

CONTENTS.

GUIDELINES STAGE 3

DETERMINING BUSINESS CONTINUITY STRATEGY

COMPONENTS

1. STRATEGY OPTIONS

2. ACTIVITY CONTINUITY OPTIONS

3. RESOURCE LEVEL CONSOLIDATION

DETERMINING BUSINESS CONTINUITY STRATEGY

Reference: BS 2999-1 Section 7

1. Introduction

The first section 'Determing BC Strategy' looks at the general issues of ensuring the protection of the ability of the organisation to deliver a product or service within its Business Continuity programme. The following section 'Activity Continuity Options' describes the tactics available for ensuring the continuity the activities that support the delivery of those products or services.

It also makes sense, where possible, to implement measures to reduce the likelihood of incidents occurring or to mitigate the impact should they fail. However no guidance can be offered here on their cost-effectiveness and they should not be seen as a substitute for the implementation of appropriate BC strategies described below.

In the previous stage the Maximum Tolerable Period of Disruption was discovered for each Product and Services within the scope and, by understanding their interdependencies this will have enabled the MTPD of each activity to be determined. Within the Strategy stage the Recovery Time Objective for each activity needs to be set within that MTPD.

DETERMINING BUSINESS CONTINUITY STRATEGY

Reference: BS 2999-1 Section 7.2

1. Introduction

This section looks at the various high level strategies available to protect product and service delivery.

2. Precursors

A current BIA is a requirement before an appropriate strategy can be selected

3. Purpose

The purpose of this step is to ensure that the overall continuity strategy appropriately supports the delivery of the organisation's product and services.

4. Concepts and Assumptions

Recovery Time Objective

When recovering an interrupted activity the organisation probably will not want to reach this point in time at which it will just survive - it may want to set a (shorter) Recovery Time Objective (RTO) that also gives it a margin in case of unforeseen difficulties with recovery or if its original measurement of MTPD was optimistic.

Continuation or restart capabilities need to be realistic. Physically moving staff and operations will take more time than expected and impact on the available working day. It is important to allow sufficient continuation/restart time into the expected to ensure that business activities can be resumed within the Recovery Time Objectives (RTO).

It is usually the case that the faster the recovery requirement, the greater the cost of a solution therefore, to minimise costs, it is important to ensure that an appropriate, but not excessively rapid, RTO is set.

Separation distance – what is off-site?

Since the BC events against which we are planning frequently result in loss of access to or destruction of a location it is necessary to ensure that electronic and other records are duplicated at another geographically separated location in a form that allows them to be accessible and recovered for use within business-defined timescales.

Whilst it is self-evident that greater geographical separation decreases the likelihood of two sites being affected by the same incident, there is no 'minimum' or 'correct' distance for separation as the ability of worldwide infections and computer viruses to cause concurrent

incidents demonstrates. However a few hundred metres is likely to provide little protection even in localised incidents because of the way that emergency services use cordons and the likely disruption to transport. Some organisations can use their market or jurisdiction area to define the limit of their dispersion (see discussion of survivable incidents in the Introduction to Stage One); others may choose the pragmatic alternative of placing a relocation site within the limit of how far they judge their staff would travel (which may be about 1 hour away).

Resilience

This term is used to indicate that something can suffer a failure and yet still continue operations. However it is often used as if it were an absolute (e.g. This computer is resilient). However, like the words 'near' or 'far', the term resilience is a relative one whose scope needs to be qualified at each use. This is best illustrated by examples:

- the addition of RAID technology to a computer increases *machine-resilience* (but only to hard-disc failures) and does nothing to protect against loss of that machine in a fire

- duplication of power feeds to a site increases *site-resilience* to power interruptions but the site can still become unusable if the power failure affects both supplies

- Expanding the geographical dispersion and diversity of the organisations locations increases *organisational-resilience* though it may still succumb to widespread incidents such as pandemics or computer viruses.

5. Process

Using the results from the Business Impact Analysis note the Maximum Tolerable Period of Disruption (MTPD).

- Decide on a Recovery Time Objective (RTO) for the product or service, which should (of course) be shorter than the MTPD. This may take into account the confidence one has in the accuracy of the MTPD.

- If there is an existing resumption strategy conduct a 'Gap Analysis' to identify where existing performance is measured against the required performance.

- Provide executive management with a strategic evaluation.

- Ensure the agreed option is 'signed-off' by the executive management including the financial and resource provisions.

6. Methods and Techniques

Issues with specific business services:

- Call Centre (s): A convergence of IT, voice recording and intelligent telephony in a call centre may provide significant recovery challenges. Call Centres handling incoming calls will usually have MTPD measured in hours rather than days so two or more centres

geographically dispersed which load share the calls are the usual solution. Due to the typical staff make-up of this type of facility during a sustained period of outage this can present manpower challenges in the event that staff are unwilling or unable to relocate. Some service companies can provide call answering with varying abilities to handle call volumes at varying level of product competence.

- **Electronic Commerce and Internet / Intranet** strategies will have a choice based on how the whole organisation views the importance of these services and the role they play - whether for communication only or for interactive business.

    ♦ the resumption parameters of Electronic Commerce Services need to be determined by a Business Impact Analysis in the same way as other functions. Electronic Commerce Services are often seen as needing rapid resumption because of their visibility and customer expectations.

    ♦ the Internet and Corporate Intranet may also provide an excellent vehicle for communications during an incident.

- **Manufacturing solutions**

    ♦ Geographical diversity - manufacturing at more than one site increases resilience to a variety of events but is usually at the expense of economies of scale

    ♦ Subcontracting - Though each company's total process may be unique, there are usually various processes which can be duplicated by other manufacturers. The affected company can then use a number of subcontractors to produce the usual finished product whilst their own facilities are unavailable. This can rarely be achieved quickly without advance preparation due to the need for tooling and set-up. Unfortunately this strategy may introduce your customers to your competitors.

    ♦ Warehousing stock - For products that can be stored, an off-site stock can provide a time window in which supply can be maintained while a disruption is resolved.

7. Outcomes and Deliverables

This step will provide an strategy for each product and service under the BCM programme that will allow the appropriate alternatives for each activity to be selected in the next step.

8. Review

A review of the BCM Strategy for each product and service should be carried out at least every 12 months. However, events may prompt re-examination of the BCM Strategy such as:

- A Business Impact Assessment revision that identifies substantive changes in processes

and priorities.

- A significant change in one or more of the following: the organisation's risk attitude (perhaps prompted by an event), market conditions, acquisition or merger, new products or services, regulatory or legislative requirements

ACTIVITY CONTINUITY OPTIONS

Reference: BS 2999-1 Section 7.3-8

1. Introduction

This step covers the process of selecting appropriate tactics for each activity supporting the delivery of one or more products and services within the scope of the BCM programme.

The Business Impact Assessment (BIA) will have identified the MTPD of each activity. Within this time the Recovery Time Objective (RTO) for each activity needs to be set.

Appropriate tactics for each activity must be selected to cover the required resources in the areas of:

- People, skills and knowledge

- Premises

- Technology

- Supplies

- Stakeholders

The options described below are not exclusive of each other. A viable and effective recovery strategy for each activity will need to be built up from elements of all options described.

2. Precursors

The RTO of the product or service needs to be determined before the RTO for each activity is set and the appropriate tactics selected.

3. Purpose

The purpose of this step is to ensure that the tactical continuity options for each activity appropriately support the delivery of the organisation's products and services.

Activities whose resumption is most urgent may be further protected by various threat reduction measures that seem appropriate.

4. Concepts and Assumptions:

Reliability

There is often a management decision to be made between the cost and reliability of delivery of a third-party service required for recovery. Promises may varying from word-of-mouth, through 'best endeavours' to a contractually committed service level. Costs may vary (usually

correlated to the quality of the promise) from nothing to a substantial sum. The tighter the RTO, the more important the reliability of the delivery becomes.

Extent of planning

The extent and detail to which the tactics for each activity need to be planned will depend on the urgency with which they are required and the complexity of the requirement.

Costs vs. benefits

It is impossible to judge the appropriate cost of measures through conventional cost-benefit analysis since this requires questionable assumptions to be made on the likelihood of incidents to demonstrate the benefit side of the equation.

Manufacturing and service industries who supply other businesses may be able to demonstrate increased sales or better margins can be achieved by demonstrating BCM capabilities (i.e. improved reliability) to their customers - and thus show a benefit to be compared to costs. This is more difficult to demonstrate when the service is non-commercial or is being provided to the public where cost savings on internal processes (reduced disruption) are more likely to be demonstrable.

Syndication Ratios of third party recovery sites

- "Dedicated" work area where a subscriber has exclusive use of accommodation. This is generally used where a rapid RTO is required, for high value-generating functions, where specialist equipment is used or where the non-availability associated with syndicated space is judged unacceptable. An example would be dealing desks for an investment company.

- "Syndicated or Subscription" work area where a subscriber pays for the use of accommodation provided that it is not already in use by a prior invocation by another subscriber.

  - The general industry ratio is a maximum of between 40 & 25 to 1 i.e. each desk is sold a maximum of up to 40 times, but great care should be taken to understand who are the other customers potentially using each desk e.g. some suppliers provide client details by post code. The parameters acceptable to an organisation should be clearly defined within its BCM Resource Recovery Strategy and should not be left to individual contract negotiations.

  - At the current time there are two basis on which a recovery supplier may allocate the available resources to subscribers during a concurrent invocation:

    - First come, first served: The first subscriber to invoke the service gets their full allocation of resource; any remainder is available to subsequent subscribers

- Equitable share: The available resources are allocated in proportion to the resources subscribed to.

Exclusion Zones (Third-party recovery sites)

The exclusion zone is the distance within which the recovery supplier will not resell the resources you have subscribed to another potential customer. The organisation's definition of exclusion zones should be clearly defined within the corporate BCM Strategy e.g. within the City of London a 800 metre exclusion zone (vehicle size bomb) is a minimum acceptable standard for this specific threat but may not be appropriate for other types of incident.

4. Process

The process includes the following steps:

- Identify possible tactics for each activity that can meet the RTO.

- Select the most appropriate based on cost, guarantees, additional benefits and other factors

- Create and an implementation project for the measure selected.

- Implement an on-going process to ensure the Activity level BCM tactics are reviewed.

Select appropriate tactics from those below.

People, workforce, skills and knowledge

Reference: BS 2999-1 Section 7.3

Techniques for the protection of the organisation's knowledge and skills and can provide some protection against loss or absence of key staff

- Process mapping and documentation - to allow staff to undertake roles with which they are unfamiliar

- Multi-skill training of each individual

- Cross-training of skills across a number of individuals

- Succession planning

Additional skills may be available by permanent or occasional use of third party support. Reliance on this support should be backed by contractual agreements.

The organisation should be protected by a knowledge management programme, which should utilise off-site storage for protection of data.

An organisation could conduct an inventory of staff skills not utilised within their existing roles.

These may include:

- First-aid training

- Experience in other roles from other employment

- Salvage

- Leadership or management of a previous incident

- Training or acting skills - to assist the Business Continuity team

Geographical separation of individuals or groups with core skills can reduce the likelihood of losing all those capable of undertaking a specific role

Premises

Reference: BS 2999-1 Section 7.4

The RTO is the principal determinant of the appropriate work site continuity tactics.

- An RTO of several months may allow the organisation to chose to leave any decisions until after the event.

- An RTO of over a day or two may allow time for staff to be relocated to another site

- An RTO of less than a day will require tactics that enable the activity to be taken on by staff at other locations - which implies the immediate availability of the resources required by that activity at the other site including current information

Once the RTO parameter has been satisfied, cost and availability will guide the choice of tactics.

The organisation's geographical spread may influence the choice of alternative facilities. Though other company locations may be preferred, staff may be unwilling to travel that distance.

A site with a large number of staff may require more than one alternative location to provide the required capacity. The organisation's future location strategy could be influenced by the availability of suitable nearby in-house alternatives or of third-party sites.

Organisations that provide services to a particular locality, such as public bodies or businesses serving a local market, may be constrained in their choice of alternative locations by the need to be close to their customers.

Work site facility tactics include:

Do nothing
- a '**do nothing**' strategy may be acceptable for the least urgent activities identified in the

BIA. Where the organisation has identified that an activity has a RTO greater than a few months this gives times time for buildings to be found and utilities to be installed post-incident with minimal planning and preparation. This option might be made more rapid or reliable by maintaining a current register of suitable buildings available.

Tactics involving relocation of staff to other sites

- **Budge up** makes use of existing in-company accommodation such as a training facility or canteen to provide recovery space or increasing the office density. This will require careful planning and some technical preparation.

- **Displacement** involves the displacing staff performing less urgent business processes with staff performing a higher priority activity. Care must be taken when using this option that backlogs of the less urgent work suspended do not become unmanageable.

- **Remote Working** includes the concept of "working from home" and working from other non-corporate locations e.g. hotels (Internet Cafes should not be considered). Working from home can be a very effective solution but care must be taken to ensure Health and Safety issues are addressed and sufficient dial-up capacity is available.

- **Reciprocal agreements** can work in some selected services but care must be taken when establishing this type of agreement. Procedures must be in place to ensure that periodic checks are performed to ensure that the required arrangements have not changed. Reciprocal agreements must have a clause in the contract to ensure that testing is allowed.

- **Third party alternative site** arrangements from a commercial or service company may be an option for consideration if these can ensure the organisation's recovery time objectives (RTO) are achieved. There are a range of commercial services including fixed, mobile and prefabricated sites.

    - Dedicated space provides guaranteed and immediate availability but is more expensive than syndicated space.

    - Syndicated space usually provides access within 4 hours but may take more than 48 hours for a large number of staff to become productive from the site *(Issues with syndication are discussed under Concepts)*

    - Mobile facilities can be in use rapidly but provide limited space and may require service connections and significant preparation of foundations

    - Prefabricated units take a minimum of 4 days to build (average 8) assuming pre-prepared foundations and depending on site and weather conditions

Diverse locations - moving the activity (not the staff)

- **Resilient Operations** include dual site operations and continuous availability solutions. In the event of an interruption at one site the business activity is transferred to one or more alternate locations at which staff and facilities are already prepared to handle it.

These options are normally amongst the more expensive to implement (due to the costs of synchronising data at multiple sites and the overhead of supporting multiple sites) but provide the appropriate solution where quick (less than 24 hour) resumption is necessary. To be a viable recovery strategy this configuration should have no single points of failure and an appropriate geographical separation and diversity of the two or more sites.

Figure: Summary of Relocation Strategies against recovery time

Ownership	In- house	Contracted	Ad-hoc
Months	• Rebuild or relocate	• Extend commercial recovery site contract (if permitted)	• Rebuild, Rent or Purchase
Weeks	• Prefabricated buildings on site • Adapt buildings from other uses	• Expansion at Recovery Site • Contracted prefabs and mobile units	• Furnished Offices • Subcontract processes
Days	• In-house Recovery Site • Budge-up • Home-working	• Commercial recovery site • Reciprocal Agreements • Mobile facilities • Subcontract processes	• Managed Offices (if available)
Hours	• Diverse locations with staff redeployed from other tasks	• Relocate a small team ONLY to contracted commercial recovery site*	• None
Immediate	• Diverse locations for each activity	• Initiate contracted 'switchover' of IT only at commercial recovery site	• None

Access is available within a few hours but logistics and welfare issues make it unlikely that operations can be resumed reliably within a day or two.

Supporting technologies

Reference: BS 2999-1 Section 7.5

Data Centre (s)

The cost of the solutions and the widespread and rapid impact of the loss of a data centre can have a major financial impact on an organisation.

There are a number of options that can provide a suitable solution including in-house resilience, recovery or third party support.

• Technology Duplication at separated locations is required when resumption timescales are tight, but increases in expense according to the degree of duplication.

- Technology Recovery provides replacement through third-party contracts

The decision as to whether to duplicate or contract hardware in advance or acquire post-incident must take into account the expected lead-time for acquiring the items in a widespread incident that may be long when less-prepared organisations may be chasing the same equipment. Verbal promises by a supplier to keep a contingency stock should be treated as non-contractual.

There is often a budget conflict between:

- the desire to increase machine-resilience (to minimise downtime due to failure of that machine)

- the need for geographical diversity (which minimises the downtime when the machine, or the building it is in, does fail).

'Ship in' Contracts

This can include generators, IT equipment such as PCs, servers and printers and specialist hardware and equipment such as telephony systems. This may be an appropriate strategy if an unprepared building is to be equipped to provide an appropriate working environment. Most ship-in contracts permit the delivery location to be nominated at invocation, allowing a more flexible response to a specific incident compared to a fixed site recovery capability. Contract terms vary from 'best efforts' to guaranteed delivery.

Telephony

The unplanned redirection of telephony to alternative locations may not be possible within an acceptable timescale particularly during wide-area events. Most telecommunications operators will offer, for a charge, a range of flexible planned solutions that will allow instantaneous or rapid redirection of calls from one site to one or more alternatives. The logistical problem of handling telephone calls during an interruption, once they have been redirected, needs to be addressed.

Techniques include:

- Broadcast notification to staff and other stakeholders

- Non-geographic numbers

- Call diversion

- Resumption plan

- Managed network services

- Mobile switchboard

- Site resilience

- Network resilience

The convergence of telephony and data networks VOIP (Voice over IP) creates new opportunities and continuity issues since telephones and e-mail are often used as alternatives if one fails, These issues need to be assessed and the risks and impacts thoroughly analysed.

Manufacturing equipment

Few options exist for third-party provision of 'ship-in' manufacturing equipment following its breakdown or loss yet there are often long lead-times on its replacement.

- Possible techniques to consider are:

- Asset restoration firms may be able to restore the equipment after damage by fire or water

- On-site maintenance or maintenance contracts with firms in the vicinity (to minimise travel delays)

- Use of local subcontractors or competitors with similar equipment

Information

Reference: BS 2999-1 Section 7.6

Just because an incident occurs it does not mean that regulatory, statutory or business standards for information management are suspended. Key issues to address are:

Confidentiality

Measures should be taken to ensure that the required level of confidentiality of data is maintained in circumstances such as:

- damage at a location - for example, an explosion may result in the scattering of documents into the street

- successful hacking, which could expose information over the Internet

- use of temporary staff

- sharing temporary accommodation with other organisations

Integrity

- Unless back-ups are taken at the same time across multiple connected systems, when restored the data may lack integrity across the various datasets. For example a new order may be present on the order database but the corresponding new customer may not be on the customer database if that was backed up earlier. Time should be allowed within the Recovery Time Objective to allow data issues to be resolved in case they hamper user recovery.

- Partial destruction of paper records may hamper recovery where it is uncertain what is missing

Availability

- Information required to rebuild equipment or recover and run business processes will need to be available at the time needed to achieve the resumption timescale

- There may be statutory requirements for access to documents or data within a specific timescale following enquiries by the public or authorities

Currency

The appropriate back-up strategy for a data set is determined by:

- The amount of data that the users can cope with without fatally hampering their ability to resume their processes

- The impact of the loss of data where the users are outside the organisation - such as customers or regulators

- The speed at which the data can be made available for use after resumption. Data back-up regimes are often designed to minimise back up time; during recovery the speed of restoration is more important. For example logging incremental (daily) changes minimises back up time; differential (changes since last full back-up) takes longer to back-up but is quicker to restore.

- There are many methods of data replication across computer systems. These include:

    - Mirroring - theoretically zero data loss

    - Shadowing - minimal data loss

    - Logging - data loss measured in minutes

Each has characteristics of potential data loss, costs, operational distance and reliability that should be compared with user requirements.

Remote storage of duplicate records (paper and electronic)

- **Paper records storage** solutions include off-site managed document stores and optical (scanned) copies.

- **Electronic record storage** can be managed in-house but are also provided by a range of suppliers (often called data vaulting). Records can be sent off-site by physical collection of storage media or by electronic transmission.

- The storage site should be sufficiently far away to ensure that the facility is not also affected by an incident, but not so far that access takes so long that RTO's are threatened. Some papers may be work-in progress and be required in short timescales whilst other may be archives retained for legal or regulatory purposes for which deep storage, at lower cost, will be suitable.

    - 'Fire-proof' cabinets may be used but do not provide acceptable protection for single copies - even if the contents survive the incident, the safe may not

be accessible.

♦ the original of some documents may be the only one legally acceptable.

Equipment and supplies

Reference: BS 2999-1 Section 7.7

The organisation needs to determine what equipment and supplies are required and how quickly they need to be available following a disruption to meet the RTO of the activity.

Techniques for equipment replacement include:

- Storing additional supplies at another location -

    ♦ if the supplies degrade over time (e.g. paper) then they should be rotated with regular stock

    ♦ changes in the process may require the stored supplies to be changed (e.g. headed stationery if the address or contact details change)

- Arrangements with third parties for delivery of stock at short notice

- Diversion of just-in-time deliveries to other locations

- Holding of materials at warehouses or shipping sites

- Transfer of sub-assembly operations to an alternate location either in-house or to a sub-contractor

- Holding of older equipment as emergency replacement or for spares - at an off-site location

- Specific risk mitigation strategies for unique or long lead-time equipment - where possible outdated equipment should be replaced otherwise its updated replacement may threaten recovery times

- Geographical diversity of processes where the RTO cannot be met by replacement if all equipment is lost in an incident

Techniques for reducing the impact of supply interruptions include

- Dual or multi-sourcing of materials

- Inspection of supplier's business continuity plans and test performance record and may include a requirement for certification against BS 25999

- Holding inventories off-site - at another site or at the supplier's site

- Significant penalty clauses on supply contracts (though this will not protect against bankruptcy)

- Identification and pre-acceptance of alternative suppliers

Stakeholders, partners and contractors

Reference: BS 2999-1 Section 7.8

There may be many individuals and groups affected by an incident. For example in a major fire at your site there may be contractors injured, local residents evacuated from their homes and local business having to close for safety reasons or suffering reduced trade. The organisation's level of responsibility (both legally and morally) for these groups should be understood.

The organisation should ensure these various stakeholder's need are satisfied or they may impede the subsequent recovery effort. For example, the local residents could press the local authorities to refuse you permission to rebuild on the site following a fire.

Civil emergencies

Reference: BS 2999-1 Section 7.9

The organisation should be familiar with the procedures of the local emergency responders.

Contact with these groups in advance may provide useful information to assist in an incident such as:

- Recommendations for suitable assembly points and evacuation routes

- Notice of specific hazards in the vicinity

- Likely position of any traffic cordons (in major settlements these may be predefined because of the pattern of the road network)

- Special access arrangements

- Participation in exercises

Civil emergency responding organisations should conduct their own Business Continuity programme to ensure that disruption to their facilities does not hamper the response service they provide to the community. In the UK this planning is a statutory requirements and local government is required to provide BC guidance to commercial and voluntary organisations within their jurisdiction.

Specific threat reduction measures

The BCM manager should be familiar with a number of threat reduction techniques that can provide protection of business activities against certain types of disruptions. Risk assessment may be used to justify which measures are adopted. They include:

- **Physical security** - Advice can be sought from the various national and international professional security associations, many who publish guidelines and best practice.

- **Information security** - Advice can be sought from the various national and international

ICT and Information Security bodies. ISO 17799 and ISO 27001 would also provide valuable guidelines to follow.

- **Monitoring systems** may provide prompt warning of utility failures, equipment failures and destructive threats

- **Uninterruptible Power Supply** (UPS) and back-up generators can protect buildings or specific equipment from power failures. They need to be maintained and tested regularly to ensure performance when required. There are also specialist recovery contracts that will supply portable generators either as a contracted service or on demand (subject to availability).

- **Sprinkler and Fire Suppression** systems are often advised for buildings with high loading of flammable materials or expensive equipment. Whilst water can put out fires effectively, it can cause considerable damage to papers and electronic equipment whether released correctly during a fire or incorrectly when triggered maliciously or by an explosion or earthquake.

Impact mitigation measures

- **Insurance**, when properly arranged, can provide financial compensation for loss of assets, increased costs of working and protection for associated legal liabilities. However it may not provide cover for the full expense of an incident or damage including the loss of customers, impact of shareholder value or loss of reputation and brand image. The BCM should work closely with the Insurance Manager to dovetail insurance cover with BCM parameters,

  ♦ An 'All Risks' type Policy will compensate for the assessed value of the damaged or lost physical assets and electronic records.

  ♦ Business Interruption insurance may pay for either the "increased cost of working" during resumption or for 'loss of profits' over the disrupted period.

  ♦ 'Keyman' insurance may provide a sum following the loss of named individuals from the business due to death, injury or resignation.

  ♦ Liability insurance may provide protection for liabilities incurred including those associated with employees and third-party property and people.

- **Asset restoration** services are provided by a range of specialist companies who can often minimise damage after fire and flood to papers, equipment and buildings. These firms may provide an advance registration service and advice, as well as being available on request post incident.

6. Methods and Techniques

The tools available to select appropriate tactics include:

- Results from the Business Impact Analysis and Risk Assessment

- Cost Benefit Analysis

- Service and process mapping.

7. Outcomes and Deliverables

The outcomes and deliverables from the Activity Continuity Options step include:

- A documented selection of continuity options for each activity, agreed and 'signed-off' by the organisation's executive management.

- A project plan for implementing the agreed strategy.

8. Review

A review to ensure that the appropriate continuity options have been selected for each activity should be carried out at least every 12 months. However, events may prompt re-examination of the BCM Strategy such as:

- A Business Impact Assessment revision identifies changes in business processes or priorities.

- A significant change in the following:

    ♦ key technology, telecommunications, accommodation, staffing, service suppliers

    ♦ acquisition or merger, new products or services

    ♦ regulatory or legislative requirements

RESOURCE LEVEL CONSOLIDATION

1. Introduction

Having selected appropriate tactics for resumption of each business activity the BCM team will be required to consolidate the resource requirements, determine how to source them and implement their inclusion in the plan.

2. Precursors

The parameters for resources for each activity will be derived from the Recovery Time Objectives and the numbers or scale determined from the Continuity Requirements Analysis.

3. Purpose

The purpose of this step is to co-ordinate and provide a predetermined level of resources within a Business Continuity Plan (BCP) to enable the implementation of the continuity options selected for each activity.

This consolidation is necessary for two practical purposes:

- If resources are to be purchased then a better price is likely to be achieved with a single order rather than several smaller invitations to tender

- Co-ordinating the acquisition of resources can prevent conflicts - such as when more than one activity within a building expects to use the same alternate workspace at another site.

4. Concepts and Assumptions

Availability of solutions

It is possible that the contracted recovery services required by the business processes do not exist in the vicinity. Some organisations have decided to provide their own recovery facilities, then offer to share them (commercially) with other companies faced by the same dilemma.

5. Process

This process includes the following stages:

- Aggregate Resource Recovery requirements from the Continuity Options section

- Evaluate the costs and benefits for each options for delivering the required resources that can satisfy the recovery time objectives and scale

- Provide executive management with a strategic evaluation of the options

- Ensure the agreed options are 'signed-off' by the executive management including the financial and resource provisions.

- Create an implementation project and action plans

- Apply the agreed strategy to implement the project and action plans (including the development of Business Continuity Plans).

- Implement an on-going process to ensure the Resource Level BCM planning is reviewed.

6. Methods and Techniques

The tools used to select appropriate solutions from those listed above to create a Resource Recovery Strategy include:

- Results from the Business Impact Analysis and Resource Recovery Analysis as refined by the Process Level Recovery Strategy

- Evaluation tools for purchasing services including value-for-money and contractual terms assessment

- Cost Benefit Analysis

7. Outcomes and Deliverables

The outcomes and deliverables from a Resource Recovery Business Continuity Management Strategy include:

- A set of recovery resources and services which can be deployed under the control of the Business Continuity Plan (BCP) that provides for the restoration of acceptable functionality for business activities:

    ♦ Within their Recovery Time (RTO)

    ♦ With information recovered to within their Recovery Point Objectives (RPO).

8. Review

A review of the Resource Recovery BCM Strategy should be carried out every 12 months. However, events may prompt re-examination of the BCM Strategy such as:

- Changes in an activity's recovery requirements

- A significant change in accommodation, staffing or available technology that may provide alternative resumption strategies

- A change in the availability of recovery services in the vicinity such as closure, merger or opening of a facility

KEY BCM INDICATORS

The following are key elements of what would be expected from a mature BCM organisation

1. The organisation has formal strategies for mitigating all business continuity risks for all areas of its operations

2. The strategies mitigate the effects of, and ensure the organisation can tolerate and recover acceptably from:

- A. All continuity-related scenarios identified in the risk assessment (s)

- B. Denial of access or loss of any worksite (s)

- C. Any technology failure

- D. Any supplier or utility failure

- E. Any outsource or other business unit failure

- F. Any civil emergencies that arise

3. Following any disruption, the strategies specifically ensure the continued integrity and timely restoration of:

- A. All affected electronic information

- B. All affected physical format (e.g. paper) information

- C. All affected work-in-progress information

- D. All affected business processes

- E. All affected logistical capabilities

- F. All affected outsourced operations

4. Strategies provide for the maintenance of core skills and knowledge following any business disruption

5. Strategies provide for the acceptable timely restoration of equipment, supplies and all other necessary resources following business disruption

6. Strategies are systematically evaluated in terms of ROI (Return on Investment) or other appropriate financial measure.

7. Strategies have a demonstrably low likelihood of being concurrently affected by another business disruption

8. Strategies takes account of and manages mutual aid provided by or to other organisations

9. Strategies takes account of and manages voluntary support provided to and by the organisation

10. The following apply for the organisation's business continuity strategies

- A. The rationale for the strategy and its development approach are fully documented

- B. All are fully up-to-date and together reflect the organisation's current requirement

11. Senior management always signs off the strategies

12. The organisation's strategies each take full objective account of

- A. The results of the business impact analysis

- B. The results of the risk assessment

- C. Experience gained by the organisation and similar organisations

- D. Cost-benefit analysis

Chapter 4 of the Good Practice Guidelines examines:

Developing and Implementing a BCM Response