BUSINESS CONTINUITY MANAGEMENT

The Companion Guide

Contents

PREFACE **PAGE**

SECTION ONE: THE BUSINESS CONTINUITY CO-ORDINATOR

BUSINESS CONTINUITY MANAGEMENT

The Companion Guide

Contents

BUSINESS CONTINUITY MANAGEMENT

The Companion Guide

Contents

SECTION THREE: BUSINESS RECOVERY **PAGE**

BUSINESS CONTINUITY MANAGEMENT

The Companion Guide

Contents

SECTION THREE: BUSINESS RECOVERY **PAGE**

SECTION FOUR

GENERAL

How to Use this Guide

Introduction

This Guide is intended to provide a practical working tool to assist those involved in Business Continuity Management within your organisation.

It is important to understand that the Companion Guide is not a Business Continuity Plan. As the name implies, it is intended as a “companion” to the planning process. It provides supporting information to those involved in the planning process as well as a storage place for the plans themselves. It is not expected that the CG be used at time-of-disaster. Working plans should always be held in a manner which enables them to be easily accessed and used at time of disaster.

As a guide it provides instructional material and templates that the Business Continuity Co-ordinator can follow and make use of during their Business Continuity Management programme. Study these carefully: the detailed content of templates and task lists may not be appropriate to your business, but the overall approach should provide a basis for efficient and effective Business Continuity Management.

Blank templates and task lists are provided at the end of the guide.

About the Reader

The Companion Guide can be read and/or used by anyone within the organisation who is involved in Business Continuity Management. However, the primary readership will be the person or persons directly responsible for developing and implementing a Business Continuity Plan within their business areas. For consistency, these people are referred to throughout this guide as Business Continuity Co-ordinators (BCCs).

Scope & Objectives

The objective of the Companion Guide is to provide all those involved in Business Continuity Planning, whether as a service provider (e.g. Facilities, Information Technology etc.) or a service user (Business Area) with the necessary tools to build and manage Business Continuity Plans.

It does not:
Show individual business continuity strategies & plans
Describe business continuity solutions
List recovery team structures, memberships and responsibilities

It does:
Describe the corporate BCP framework
Outline Team roles & responsibilities
Provide standards for plan development
Contain general planning guidelines
Summarise crisis management & invocation procedures

Document Control

The Companion Guide is intended to be held by Business Continuity Co-ordinators (BCC). It should be held, securely, within the Business Continuity Co-ordinator's working environment. It should be treated as a 'Vital Record' and copied off-site.

This document is intended to provide an overview of the Business Continuity Management process, as well as help and guidance to Business Continuity Co-ordinators through their Business Continuity Planning programme. It is not intended to be used at time of disaster.

COPY NUMBER	ISSUED TO
	NAME: **BUSINESS FUNCTION:** **LOCATION:**

SECTION ONE:

THE BUSINESS CONTINUITY CO-ORDINATOR

Business Continuity Management – Overview

Introduction

This document provides an overview of Business Continuity Management. It is intended to be read by both those who are perhaps new to the subject and also those who are already familiar with the subject.

Terminology

Business Continuity Management is used throughout this document as a generic title for the process by which an organisation protects itself against both the short and long term effects of unpredicted incidents. Elsewhere, you may find the same process referred to as Business Continuity; Business Recovery; Business Resumption; or Disaster Recovery Planning. For the purposes of this Companion Guide, the term **Business Continuity Planning** will be used for consistency, ease of use and as a collective term to represent:

Contingency Planning:

The process by which incidents are notified, escalated and managed.

Recovery Management:

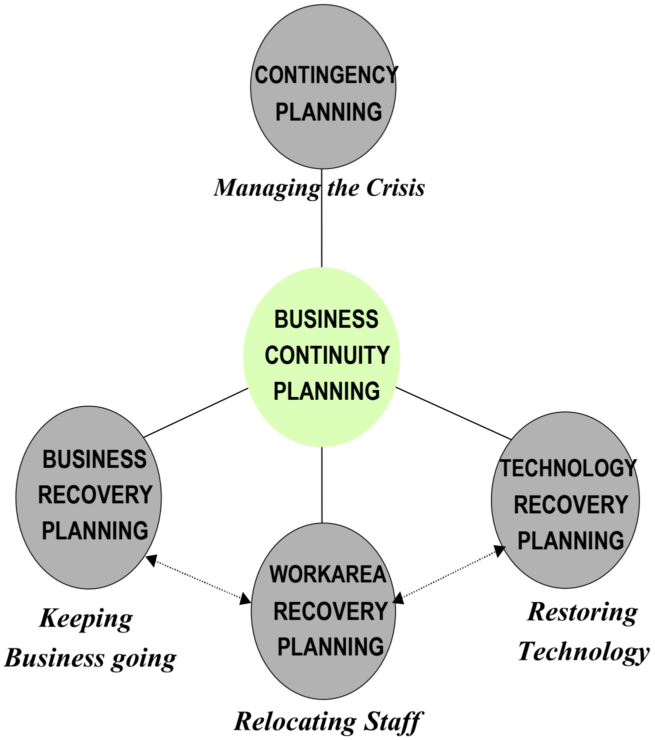
Business Recovery
The process by which Business Units rescue and recover work in progress and resume business at time of disaster.

Workarea Recovery
The process by which impacted and displaced business functions are relocated to alternate accommodation.

Technology Recovery
The process by which Information Technology services and communications are rebuilt and restored back to the users at time of disaster.

What is Business Continuity Management ?

Business Continuity Management consists of four main elements:


CONTINGENCY PLANNING
Managing the Crisis
BUSINESS CONTINUITY PLANNING
BUSINESS RECOVERY PLANNING
TECHNOLOGY RECOVERY PLANNING
WORKAREA RECOVERY PLANNING
Keeping Business going
Restoring Technology
Relocating Staff

1. CONTINGENCY PLANNING

This is the process by which an organisation plans to manage major incidents and crises. Such incidents may include, inter alia: terrorist threat/damage and other environmental disasters such as fire, denial of access, strikes, etc.

It should not be confused with Crisis Management (sometimes known as Incident Management) which refers to the actual MANAGEMENT of an incident when it takes place. Contingency Planning allows effective Crisis Management to take place – but the two processes require different disciplines, and often different personnel.

2. CRISIS MANAGEMENT

This is the process by which users are evacuated at time of disaster and describes the management of the whole process. You should note that the term ‘crisis’ is an epithet which is applied to the process and the team(s) managing this process in the first few hours following the incident. It is important that the word ‘crisis’ is dropped as soon as possible during the recovery process to give the message that the incident is being managed and is in control. As soon as the immediate incident has been safely contained, responsibility should devolve to a CONTROL GROUP, which may include personnel from both Contingency Planning and Recovery Management teams.

3. RECOVERY MANAGEMENT

This is the process by which an organisation manages its long-term recovery from an incident or crisis, to the point where business can be conducted as normal. It has three key elements, all of which may come into play in the event of a business interruption:

Business Recovery

This is the means and method by which business areas respond to an incident which has materially affected their place of work. Often leading to the relocation and reorganisation of business priorities and staff this type of planning is dependent upon the support of other non-business areas such as Property, Personnel and Information Technology.

Workarea Recovery

This is the process by which alternative accommodation is understood, prepared and activated at the time of the incident. Disrupted business often means displaced business. Such alternative accommodation may be found internally or externally. Options include:

Internal:	Unallocated space Business Continuity space Co-opted space
External:	Third-party fixed site dedicated to Business Continuity Third party mobile site delivered to suitable site chosen by client e.g. premises car park

Planning for such a relocation is essential. This is necessary to minimise:

Disruption – staff practised in relocation will recover quicker at time of disaster
Cost – keeping such space requirements down lessens the pre-usage expense

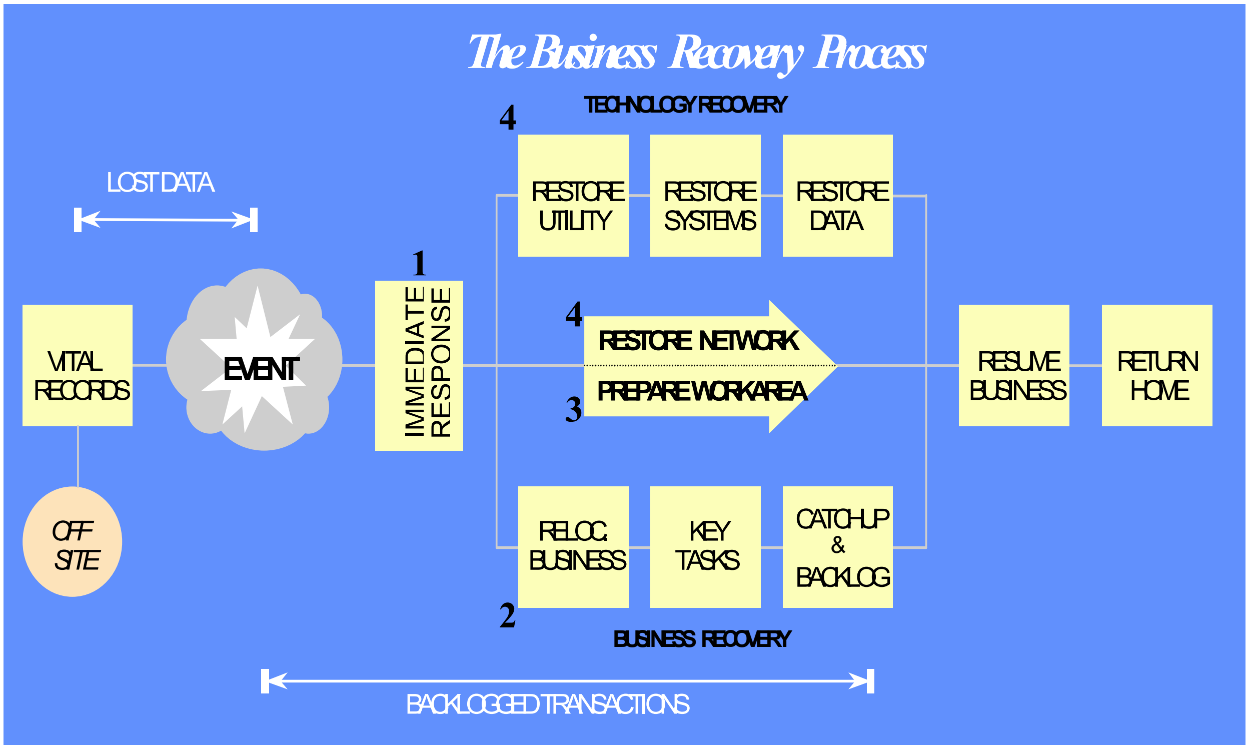
Technology Recovery

This is the process by which business manages a major Information Technology failure. Business must have plans to manage their work, resources and priorities in the event of a major interruption/failure of their Information Technology services. This aspect of planning therefore covers the situation where the business is not physically displaced but requires procedures to cope with a break in service. Technology Recovery Plans may be and often are 'wrapped' into Business Recovery Plans. The development of these plans needs Information Technology support but is the responsibility of the business to develop.

Technology Recovery is a highly specialised area, and will almost certainly require co-ordination by your internal Information Technology department or an external supplier. A detailed overview, with supporting templates, is included at the end of this section of the Companion Guide.

The Recovery Timeline

While Business Continuity Plans may in practice vary considerably in style and content within an overall corporate framework, they will largely follow a similar pattern in terms of the stages of recovery that they must address. Recovery, in most instances will reflect the following approach:



Key:

1. **Contingency Planning:** Crisis Management, Escalation and Invocation.

2. **Business Recovery:** Relocating (if required); attending to priorities; recovering lost work and catching-up on any backlog

3. **Workarea Recovery:** Preparing alternate site(s) for occupation

4. **Technology Recovery:** Resurrecting technology platforms; restoring systems and data backups; synchronising systems; communications, determine business critical processes and business systems applications.

Business Continuity Co-Ordinator – Initial Tasks

The following tasks give a suggested approach to the role in planning mode

1. **Familiarise yourself with the Business Continuity Management Companion Guide:**

- Establish reporting lines to Risk Management and Security Groups within your organisation

2. **Assess the risks to your business:**

- Arrange a Risk Assessment
- Arrange a Business Impact Analysis
- Assume worst case scenario
- Determine business critical processes

3. **Build Contingency Planning, Crisis Management, Recovery Management teams:**

- Establish team members
- Brief teams

4. **Establish and agree activities to be undertaken by Contingency Planning Team Chair and Recovery Management Chair:**

- Prepare staff call lists
- Train all members in their roles and responsibilities
- Establish reporting lines to your service providers and designated workarea recovery centre
- Discuss provision of Information Technology recovery services and facilities with your Information Technology specialists, and set up formal contracts if necessary
- Identify what needs to be classed as a vital record
- Locate suitable location away from current site
- Administer the transfer of vital records to identified location

5. **Set up timetable for development of Contingency and Recovery Management Plans and ongoing review and update**

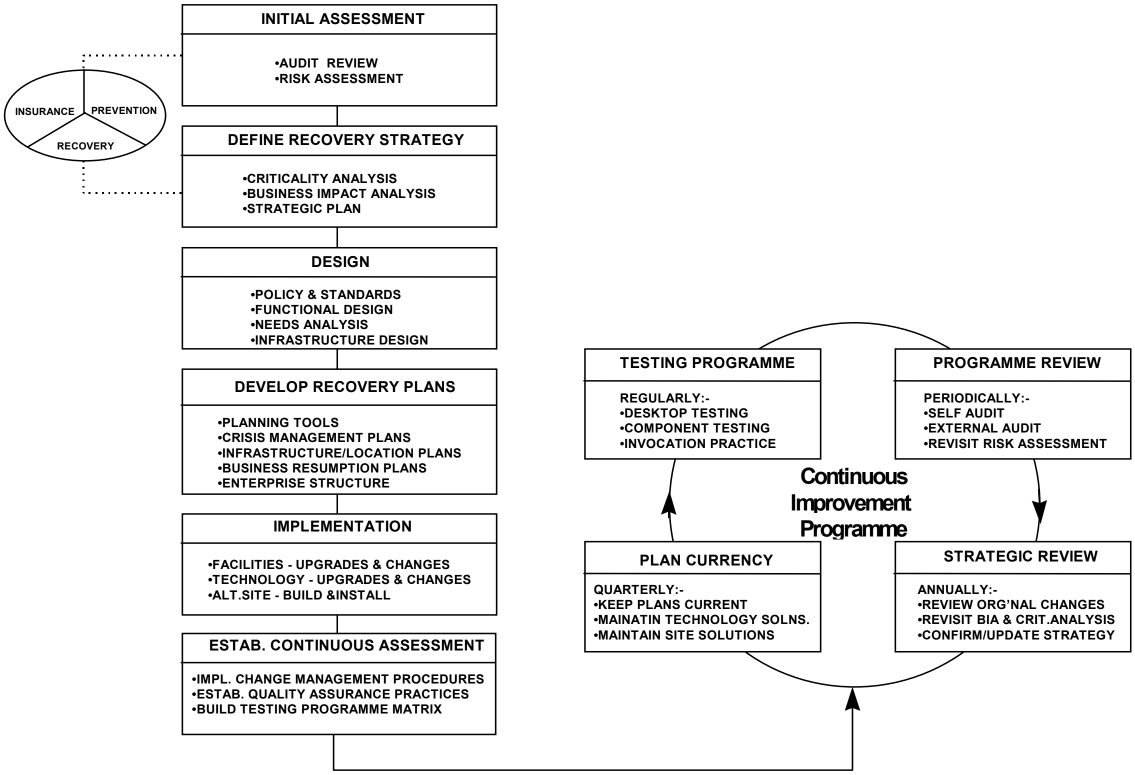
Business Continuity Plan Development Life Cycle

Business Continuity Planning consists of two major Project Management phases.

- The first, is a one time exercise to determine what is required by the organisation in terms of a recovery strategy together with the setting up of processes and procedures which will ensure that recovery strategy and solutions remain current.

- The second phase is the cyclical application of those processes and procedures established during the initial phase, so that the organisation's strategy and solution remain current.

Thus:



Risk Assessment

Introduction

Risk Assessment is the process by which an organisation reviews its operations and assesses to what extent it is at risk from incidents that may interrupt the business process. Business function priorities, once identified and communicated, must have an appropriate risk management strategy associated with them. Prevention, insurance and recovery all play key roles in managing risk. The key is to see all three as part of a physical and strategic approach to Business Continuity Management.

Consider:

1. You can't **prevent** everything, no matter how much you spend.
2. You're not **insured** for lost clients that never come back
3. **Recovery** restores business functions where prevention fails to do so and avoids what insurance doesn't cover – intangible losses.

The balancing factor is risk – how much risk is a business willing to accept? What percentage of resources (time and money) should be allocated to prevention, insurance and recovery?

Overview

Risk Assessment consists of three phases:

`Risk Analysis
Understanding threats and vulnerabilities to the business

|

Business Impact Analysis
Documenting the effects of business interruption

|

Needs Analysis
Determining minimum resources of the business

that in turn leads to:

Strategy
Agreeing a strategy to address the needs

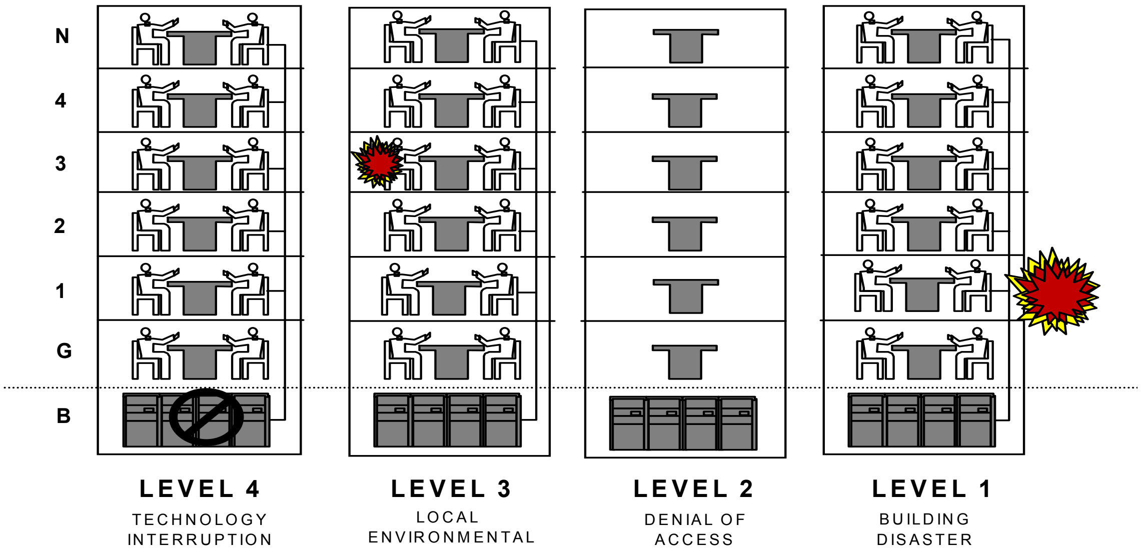
|

Solution
Implementing the strategy

Phase 1: Risk Analysis

With the support of Facilities Management and Information Technology functions assess the physical and operational vulnerabilities of the business function. Responsibility for addressing these threats generally resides with Facilities Management.

DISASTER CLASSIFICATION



Areas for Review

A structural survey should be undertaken by Facilities Management and Information Technology to report on the following:-

1. BUILDINGS AND FACILITIES

- Resilient or brittle construction
- Resistance to progressive collapse
- Internal partitions, corridors and doorways - define staff shelter areas
- Vulnerability of glazing systems, e.g. to vandals, explosion etc.
- Flood protection: natural flooding, burst water mains
- Access for Emergency Services, likely response times
- Hazardous gases, materials and processes in locality
- Location of vital internal facilities, e.g. computers, archives
- Fire protection and alarm system
- Escape routes and equipment
- Insurance for reconstruction

2. PERSONNEL SAFETY

- Quality of established emergency procedures and training activities
- Safety zones within/outside buildings, signage
- Use of protective clothing and safety equipment
- Roll-call procedures
- Post-emergency warning and communications systems
- Emergency hierarchy and command structure

3. CRITICAL ASSETS

- Software back-up, frequency & security of copies
- Key documents and information, storage & protection
- Vital equipment, without which you cannot operate
- Bespoke, unique items - alternative processes
- Obsolete, unobtainable items
- Unusual tools, measuring and calibrating devices
- Patterns and jigs
- Specifications and drawings
- Telecommunications systems, alternative feeds
- Computer equipment and networks
- Back-up power supplies
- Insurance, business re-construction and added costs

4. **SUPPLIERS AND ALTERNATIVE SOURCES**

- Sources of alternative equipment
- Availability of spare capacity Rapid supply of consumables and materials stocks
- Equipment repair and maintenance services
- Relationships and communications links with suppliers

Risk Assessment Rules:

All Business Continuity Planning:

- will be developed against a worst-case scenario, i.e that it will happen at the worst time on the worst day.
- will assume that the disaster is a major one.
- will assume that the normal location is unavailable for at least 48 hours
- will assume that there will be a core of experienced staff to recover the business

Phase 2: Business Impact Analysis

The business must assess in quantitative (financial) and qualitative (reputational) terms what the impact on the business would be if there were an interruption that lasted for 24 hours (short-term), 3 days (medium term) and 10 days (long term).

The questionnaire on the following pages is an example of this process.

The purpose of the questionnaire is to get the business to understand the likely effect on the business if there were a short, medium or long-term interruption.

Business Impact Analysis (BIA) is a very important phase in business continuity planning and unfortunately, for a variety of reasons, it is often ignored or not fully considered.

An informative and detailed BIA will clearly show the inherent vulnerabilities of the system(s) that you may have.

A good BIA will do two things: firstly it will highlight those areas of such importance and vulnerability that they should be controlled or improved to avoid the risk. Secondly it should prioritise its activity for recovery, firmly establishing timescales for key responses.

From the time of any incident or disaster, the ability of a company to survive will depend on the nature of their revenue i.e. type of work undertaken by the business e.g.

a) if they provide specialised or customised products or services where the customer cannot easily go elsewhere
b) in the commodity sales market, customers can go to another supplier, probably competitor but maybe are prepared to wait a few days to stay with ‘the devil they know, rather than the devil they don’t know’. This may be typical of insurance.
c) some companies e.g. rent collectors receive most of their revenue at a particular time of the month or year e.g. month end so depending on the date of the incident, it may have little or no immediate impact. For a policyholder whose policy is not up for renewal or currently experiencing a claim, they might see little evidence of an issue.

In the case of a) above, this customer is fully dependent upon your service and if you are not operating, then your situation will have the greatest impact on them. In b), this is likely to be customers who regularly move their supplier perhaps looking for the cheapest price or quickest delivery time but who feel no particular loyalty to yourselves. This would cause a sudden and large decline in revenue. In c), these customers will survive and stay with you and may not even be too aware of your situation.

Other issues that may cause a major impact on your business could be lost productivity leading to higher expense ratios, lost market share and lost customer confidence.

If the revenue decline was plotted on a graph the steepest graph would typically be those in the finance and banking sector, telephone sales, etc. The shallowest graph would be companies who operate in a niche market and might hold their customer base.

At the outset, it is tempting to try and group everyone together and assume that they all follow the same line and have the same needs. Every section, department or business process must be looked at individually.

Many business processes are dependent on or have a high usage of automated systems and so the impact of loss of these systems has to be reviewed. In the short term you may be able to turn their attentions to other aspects of our work when such systems become unavailable e.g. make those return telephone calls, attend meetings, write up minutes, etc. whereas some sections are unable to work once their automated systems fail e.g. telephone sales.

Phase 3: Needs Analysis

Once the impact(s) have been agreed then the process of determining what the business would require in the immediate aftermath of a disaster can be undertaken.

This is also addressed in the questionnaire.

Analysis Rules:

- Resources required within a 24-hour timeframe must be contracted for in advance. At time of disaster, many of these resources (e.g Desks, PCs etc) are not 'off-the-shelf' items in large numbers. In order to be able to occupy and use such resources within 24 hours they should be 'ready and waiting' somewhere. Facilities Management can not be expected to source and acquire these immediate needs, immediately.

- Day 1 resource requirements should be minimised.

- When planning the rate at which minimum resources grow to normal operation resources, do not use a timescale that is too discrete. Do not conduct a Needs Analysis that asks the question, how many (e.g.) PCs do you require after 1 day, 2 days, 3 days, 5 days etc. Delivery and installation of such resources is time consuming. Information Technology and Facilities Management functions who may be servicing many affected business areas, or who may themselves be impacted by the incident, can not keep coming back to your recovery site to install/deliver more equipment.

- Use the Needs Analysis to prioritise resources, spread and/or delay delivery of resources if possible.

SAMPLE BUSINESS IMPACT/NEEDS ANALYSIS QUESTIONNAIRE

Business Impact & Needs Analysis
for
Business Name

Amongst the several disastrous events that could prevent any of our operations from carrying on their business, the loss or failure for more than a few hours, of any part of our technology infrastructure calls for an effective contingency plan.

The first step in the Business Continuity Management programme is to determine and understand the impact on your business due to the unavailability (for a significant period of time) of each one of the services used by your area.

You are asked, therefore, to complete the attached questionnaire prior to a follow-up meeting with the team working on this – the Business Impact Analysis (**BIA**) - project.

The completed questionnaire(s) will be collected at the follow-up meeting. This meeting will provide an opportunity to clarify any points and helps the project team avoid any misunderstandings.

Please do not attempt to go into too much detail in your written answers: as a guide the questionnaire should take no more than 45 minutes to complete. If unsure of how to respond to a question, leave blank until the interview.

Thank you

A. Someone
Business Continuity Co-ordinator

A.N. Other
Deputy BCC

SECTION DETAILS:

Department:	Section:
Location:	Date:
Completed By:	Telephone:

Briefly describe the function of this Section:

1. **RECOVERY TIME OBJECTIVES**

Indicate the Recovery Time Objective (RTO), by inserting A, B, C, D in the appropriate column/box for each application that your Section uses. The RTO is the time you believe that the application should recommence following an unplanned and abrupt disruption.

A = SITUATION IS MANAGEABLE *(irritating perhaps but not materially affecting the business)*
B = SITUATION IS DISRUPTIVE *(some concern that deadlines are being missed and working patterns altered significantly. Potential financial/business loss)*
C = SITUATION IS CRITICAL *(business is being seriously affected, deadlines missed; penalties incurred, close to being 'closed for business')*
D = SITUATION IS DISASTROUS *(ability to continue in business is seriously threatened. In breach of legal & statutory regulations. Doors closed for further business. Long term impacts uncertain.)*

Computer Applications and Services	**✓if**	**%**	**√ when first required in an emergency**		
	used	*****	1 Day	1 week	4 weeks.
Example	✓	**50**	**A**	**C**	**D**
Business Systems					
Operations Systems					
Quality Management					
Engineering					
General Office					
Microsoft Office Products					
ANY OTHER SYSTEMS USED					

NOTE * For each application enter the amount of time your Section spends using this application as a % of its overall workload.

2. NON FINANCIAL IMPACT

Estimate the **"non financial"** impact of the discontinuance of the Section's activities to our customers, clients, Regulators, investors, etc.

Use the following scale and please mark each box:-

1= Catastrophic 2 = Disastrous 3 = Severe 4= Serious 5= Mild

Refer to the attached 'Criticality Ratings' document

LOSS CATEGORY	TIME SECTION UNABLE TO OPERATE		
	1 Day	**1 Week**	**4 Weeks**
Example	**5**	**3**	**3**
Company Image			
Company Customers			
Investors			
Regulators			
The Environment			
Company Employees			
Suppliers			
Other			

3. DISRUPTION FACTOR

Please rate your view on the level of internal disruption to the Company due to an unplanned and abrupt discontinuance of your Section's activities.

Please use the scale 1 to 5, where:-

1= Catastrophic 2 = Disastrous 3 = Severe 4= Serious 5= Mild

Disruption Factor	1 Day	1 Week	4 Weeks
Example	**5**	**3**	**2**
Your View			

4. FINANCIAL LOSS ANALYSIS

The primary purpose of this question is to establish the amount of loss the business would experience in the event of a major disruption.

In order to establish financial impact an estimate of the financial loss associated with the discontinuance of the services provided by this Section is required. When estimating the loss always assume the emergency (e.g. loss of building) occurs at the most critical period of your operation. Please indicate how often these critical periods are likely to occur. (e.g. daily, monthly, quarterly, twice yearly or other):

To assist in identifying the losses, several categories have been defined, as per the table below. In addition, to more easily assist in estimating financial loss, cumulative loss range groupings have been established. The loss ranges are:-

'$ RANGE' GROUP TABLE

GROUP NUMBER	FROM	TO
1	$0	$150,000
2	$50,001	$300,000
3	$300,001	$750,000
4	$750,001	$1,500,000
5	$1,500,001	$3,000,000
6	$3,000,001	$15,000,000
7	If greater than $15,000,000 enter amount	

On the following table give an estimate of the amount of loss in each of the time periods shown, using the Group Ranges 1 through 6. ***Note. Boxes left blank will be assumed to imply no measurable losses will be incurred.***

LOSS CATEGORY	**TIME SECTION UNABLE TO OPERATE**		
	1 Day	**1 Week**	**4 Weeks**
Example	**1**	**2**	**5**
REVENUE LOSS E.g. Lost business, loss of profits, delayed billing, etc.			
LEGAL & COMPENSATION COSTS E.g. Sanctions or fines, lawsuits, compensation.			
ADDITIONAL EXPENSES E.g. Additional manpower, overtime, equipment, materials lost.			
ANY OTHER LOSSES (Excluding loss of equipment, such as desks, chairs, PCs, etc.)			

For example, if after a 1 week discontinuance you estimate there would be a revenue loss of, say, $250,000 then you would enter 2 in the appropriate box, as per the example above.

5. RECOVERY POINT OBJECTIVES

Please indicate the data loss that is acceptable once the service has been restored. Can your business cope with data restored, for example, to the start of the business day when the service was lost or, does the data have to be restored exactly to the 'point of failure' (i.e. back to the precise time at which the service failed). You should be aware that the nearer to the point of failure that you need your data restored to, the more expensive the solution:

Point of Failure = High Cost
Intraday Recovery = Medium/High cost
Start of Day Recovery = Medium Cost
Start of Week Recovery/Start of Month Recovery = Low Cost

Computer Applications and Services	Point of Recovery				
	Point of Failure	Intraday*	Start of Day	Start of Week	Start of Month
Example			✓		
Business Systems					
Operations Systems					
Quality Management					
Engineering					
General Office					
ANY OTHER SYSTEMS USED					

NOTE *Intraday typically means that you can only tolerate a loss of a few hours work.

6. MANUAL PROCEDURES ANALYSIS

Only complete this information for applications if there is a manual back-up procedure that could be implemented in an emergency.

APPLICATION / SERVICE	√ IF	MANUAL PROCEDURES *(SEE NOTE 1 BELOW)*			TIME SECTION UNABLE TO OPERATE (*SEE NOTE 2)* EFFECTIVENESS IN 10% STEPS		
	USED	PROCS AVAIL-ABLE	PROCS DOCU-MENTED	STAFF TRAINED	1 Day	1 Week	4 Weeks
Example	✓	✓	✓		**70**	**20**	**0**
Business Systems							
Operations Systems							
Quality Management							
Engineering							
General Office							
Microsoft Office Products							
ANY OTHER SYSTEMS USED							

Notes

1 Indicate by a tick (√) in the appropriate box if manual methods/procedures are . . . . . “available”, “documented” and if employees are “trained” in their use.

2 A manual back-up procedure is considered 100% effective if it meets the minimum functional requirements of the system it is replacing. Enter the % effectiveness in the appropriate “period” column in multiples of 10%. For example; if after 1 day you estimate manual procedures would be 20% effective for an application enter 20% in the 1 day column, after 1 week 30% effective enter 30% in the next column, etc.

7. VITAL RECORDS ANALYSIS

If you are not sure of the answer leave blank.

NAME OF VITAL RECORD	TYPE OF MEDIA *	ARE COPIES …..				ARE RESTORES …..				BACKUPS ARE TAKEN ***
		BACKED UP		OFF SITE **		IN PLACE		TESTED		
		YES	NO	YES	NO	YES	NO	YES	NO	
Example	**MM**	✓		✓			✓		✓	**D**

NOTES

* Note type of Media, enter **MM** for magnetic media or **HC** for hard-copy

** When answering this question **'off-site'** means remote from the computer on which the service operates

*** Enter **D** for daily, **W** for weekly, **M** for monthly or **O** for other, enter as many as appropriate.

8. EMERGENCY RESOURCE REQUIREMENTS

Enter the requirements needed in the event of emergency procedures being implemented - assume limited resources only are available. **Only enter the resources required by your Section**.

TABLE A

Critical Tasks	Usual No. of Staff	In an emergency enter No. of staff required in		
		1 Day	1 Week	4 Weeks

TABLE B

Computer Software		In an emergency software required within		
		1 Day	1 Week	4 Weeks

TABLE C

Computer Equipment	Usual Qty	In an emergency enter Qty. required in		
		1 Day	1 Week	4 Weeks
Network PCs				
Laptops				
Stand Alone PCs				
Dumb Terminals				
Printers				

TABLE D

Office Equipment	Usual Qty	In an emergency enter Qty. required in		
		1 Day	1 Week	4 Weeks
Office Station (Desk & Chair)				
Telephone				
Cabinets				
Photocopier (Shared)				
FAX (Shared)				
Others:				

9. **COMMENTS**: *(Add any comments here)*.

Head of Department:	**H.O.D Approval:**

Technology Recovery

Introduction:

Technology Recovery is a complex and demanding discipline in its own right. The vast majority of today's organisations are Information Technology -dependant to some degree, but the platforms around which Information Technology systems are built vary considerably from business to business.

For this reason (depending on the degree of technological complexity within your business) Technology Recovery may need to be treated as a separate element within the Business Continuity Planning process – with specialist input from your Information Technology department or external suppliers.

The section that follows contains detailed planning templates that will allow you to prepare for Technology Recovery as part of your overall Business Continuity Planning. It is highly likely you will require specialist Information Technology skills to formulate this Technology Recovery strategy, but the templates are included at this stage in order to help you integrate this area within your overall plan.

There are three areas for consideration (again, depending on the complexity of your business):

- desktop systems including LANs and standalone PCs
- midrange systems
- mainframe systems

Each of these sections has its own requirements. The following pages contain detailed templates for analysis of DESKTOP and MIDRANGE systems.

However MAINFRAME systems will require highly specialised input (possibly from an external supplier) and are therefore outside the scope of this guide. If your business is mainframe-dependent, you should seek technical support from your Information Technology department or external consultants.

Technology Recovery Overview:

Business critical systems and software

The Business Impact Analysis should have already been completed and this will have identified all the business processes that take place.

The next stage is to take the outcome from that report and map the software and data that is used to support the business process.

The fact that a system or process exists does not mean that it is critical to running that department's workload. In many cases, a system is business critical which means that following an incident or disaster at the normal place of work, then recovery of that system must be undertaken within a defined time scale at another workplace on other hardware; otherwise there may be a measurable impact of failing customer service, financial loss or general embarrassment.

It is often said that if a system exists then it must be business critical. This is not always true, especially with desktop systems and LANs, as they may only be used for the test or development environment for future software or simply as a tool for word-processing.

To establish if a desktop or midrange system is business critical, complete the first two tables in the appropriate section. The first asks a series of questions including details of each software component that is loaded on the system, frequency of use, whether the original software disks are available or a backup, if the software is essential in enabling the department to provide its service or just useful/nice to have, etc..

The second table requires all data files to be listed as these are the working files containing customised data and information. This can best be achieved by listing the lowest directory name and an indication of the type of file e.g. work processing, spreadsheet, database, etc. and whether backups are taken.

Questions & Prompts

To assist in the total preparedness of disaster recovery planning for the applicable systems, a series of questions and prompts have been prepared.

These cover many aspects for consideration in the planning phase and to each question a yes/no response is required. If the response falls in a shaded box, it may indicate that further preparations are required/need to be considered.

Each question refers to the appropriate template which should be completed as this will finally define the disaster recovery requirements for the desktop or midrange system (as appropriate) which can then be discussed with Information Technology Services.

Responsibilities

The responsibilities of the business, systems administrators and Information Technology Services are detailed in a table along with the main disaster recovery planning and recovery tasks.

While many tasks are clearly the responsibility of one department, it will often require discussion and planning with other teams.

Next Steps for Desktop and Midrange

Please complete the Tables in respect of your self assessment of critical exposures.
You may need to consult your Desktop Support and Midrange providers in order to complete the tables.

DESKTOP SYSTEMS

RECOVERY PLANNING TEMPLATES

Define all the software in use on the desktop system or LAN

If you consider all the software and data that is in use on the desktop system or LAN, then this will help to cross check and confirm the results of the BIA. This should include infrequent usage software and data files as well as everyday ones. The provision of version and licence number gives the component uniqueness to your environment.

Business Process Or Function	Software Product	Version Number	Licence Number	Operating System ✓ or x	Commercial or bought in software ✓ or x	Linkage Software To other products or services ✓ or x	Frequency of use d= daily w= weekly m= monthly etc.	Essential ✓ or x	Useful or nice to have ✓ or x	Backup or original disks ✓ or x	If software on server, how many Staff have Access to that server

Define all the data files stored on the desktop system or LAN

This list should contain all the data files that are in use and should include infrequent usage files well as everyday ones.

Business Process or Function:	**Directory name:**	**Essential ✓ or x**	**Useful or Nice to have ✓ or x**	**Backup taken ✓ or x and frequency**	**Word Processing ✓ or x**	**Spread sheet ✓ or x**	**Database ✓ or x**	**Other ✓ or x**

A desktop system or LAN can be deemed business critical if you have a tick in any of the boxes in the above two tables indicating essential. You must ensure that, if not already being done, backups of those files marked as critical are regularly backed up and stored at the designated offsite vital records store.

The business critical desktop system or LAN must now be defined in more detail; only give details of what is essential to be on the system. These requirements will define the key elements of the system which is to be recovered as soon as possible after the disaster or incident.

Non-essential, useful or nice to have systems or data can always be recovered at a later time.

Desktop Continuity

In answering the questions below, any response that falls into a shaded box may mean that the disaster recovery preparedness of your desktop system is not complete and may indicate that further preparations have to be considered.

		YES	NO
Acceptance Tests	Have you prepared a series of short tests to run when the desktop system is recovered to check that it is functioning ok & all systems/transactions/data are available ?		▨
Acceptance Tests	Have you prepared a series of short tests to run when the desktop system is recovered to check that printers & any special connections are working ?		▨
Access Control	If any/all of your systems/files/processes password protected, could you foresee any situation where a critical password may not be available so hindering/preventing progress of the recovery ?	▨	
Access Control	If yes, do you keep a set of emergency passwords at the vital records store (provided it is secure enough) ? If so, where is your store?		▨
Backups	Do you keep your backup disks/tapes offsite from your work location ?		▨
Backups	Do you have a different backup routine depending on the day of the week, the week in the month and/or the month in the year ?		▨
Backups	Is the backup restore procedure documented ?		▨
Backups	Has a restore/recovery of the backups been undertaken to test that the backup procedure has been done correctly ?		▨
Backups	If so, did you encounter any problems ?	▨	
Backups	Has a restore/recovery of the backups been tried to equipment different to that which you normally use ? When was this done, by whom and where?		▨
Backups	If so, did you encounter any problems ?	▨	
Backups	Are there any system requirements or defaults that must be in place prior to commencing the restore/recovery from backups ?	▨	

Configuration	Have you documented the minimum specification for the system ?		▨
Configuration	Are all/any system configurations detailed so that a competent technician could rebuild it ?		▨
Dependency	Does this system require any other software or hardware outside its normal environment to be available for it to function ?	▨	
Desktop including LAN	Have you completed the Desktop DR Templates document and discussed your requirements with the Information Technology LAN DR providers team ?		▨
Hardware & Software	Do you have a complete list of all hardware and software installed on your system(s) ?		▨
Hardware & Software	Has this list of hardware and software been reviewed in the last three months ?		▨
Hardware & Software	If you need additional hardware and software to be obtained and installed at the recovery site, can it be achieved in the timescales required ?		▨
Hardware & Software	Do you require connectivity to other systems/services e.g. mainframe, BACS ?	▨	
Hardware & Software	Is this connectivity requirement documented ?		▨
Hardware	Do you have any customised equipment that cannot be purchased/replaced off the shelf ?	▨	
Hardware	Have you considered the impact on your business if you do not have this customised equipment ?		▨
Invocation	Do you know and have documented the invocation procedure for LAN DR ?		▨
Recovery Time	Do you have a documented timetable for the order and timings that any recovery/restore will take ?		▨
Salvage	If your hard-disk became unavailable, have you considered the implications of not being able to get access to it, either in the short or long term ?		▨
Salvage	In your recovery time plan, have you considered that, although your PC/hard-disk is available, specialist checking may be required before you are allowed to recommence using it (e.g. if taking from incident site) ?		▨
Security	Do your system(s) have any confidential or sensitive data or information on it that may require special considerations when running at another site ?	▨	

Software	Are you running any software that is not longer supported by the supplier and may therefore cause problems when installed in a different environment ?	▨	
Software licence	Is a new licence required for change of hard disk running environment ?	▨	
Software licence	Do you have and know where to locate the original software licences?		▨
Standalone PC/Desktop	If you have any Standalone PC/Desktops, are they as delivered from the supplier to the standard specification ?		▨
Standalone PC/Desktop	If no, have you the specification of what this system now contains ?		▨
Standalone PC/Desktop	Is this information held in the vital records store ?		▨
Technical Manuals & Documentation	Does the recovery centre have the technical manuals for the equipment installed and basic operating systems ?		▨
Technical Manuals & Documentation	Are all your system procedures documented and copies kept offsite or at the vital records store ?		▨
Vital Records	Have you made up a disaster recovery box containing recovery procedures, etc ?		▨
Vital Records	Is the disaster recovery box kept at the designated vital records store or offsite ? Where is this ?		▨

Responsibilities of Information Technology Services and the Business

Recovery responsibility:	Business	IT LAN Administrator	IT Services or Local PC Support
Establish if LAN/desktop is business critical	✓		
Identify number of servers, workstations, printers, etc.	✓		
Establish backup strategy	✓		
Establish recovery timetable and prioritise recovery	✓		
Saving files on server	✓		
Backing up server to disk	✓		
Recover LAN server and workstation(s)		✓	✓
Connect workstation(s) to LAN			✓
Install/configure any additional connectivity hardware e.g. modems		✓	✓
Set up printer and produce test output to confirm recovery/connectivity		✓	
Negotiate disaster recovery contract with third-party			✓
Provide list of authorised business personnel who can request LAN disaster recovery service	✓		
Request LAN DR recovery service	✓		
Invoke contract			✓
Co-ordinate LAN DR recovery			✓
Provide LAN technical support			✓
Co-ordinate business recovery	✓		
Document business process	✓		
Obtain hardware quote/contract for any hardware not met in third party contract			✓
Provide NDS information e.g. treenames, startup/autoexec files, etc.		✓	
Write business recovery plan	✓		
Write desktop/LAN disaster recovery plans		✓	

Sensible Preventative Measures & Housekeeping

- Protect your desktop from unauthorised use.
- Protect your desktop and diskettes from unauthorised removal.
- Only use, and allow to be use on your desktop, software which has been acquired through approved procedures.
- Scan all incoming diskettes for viruses prior to using them on your desktop.
- Scan your hard disk regularly and frequently depending on how much you use your desktop.
- Do not load ‘shareware’ or bulletin board software’ on your desktop.
- Take regular copies of the software and data on your desktop; either backup onto the server if on a LAN or store diskettes at offsite vital records.
- Don’t keep old or no longer required files especially word processing letters etc.
- Keep test files to a minimum.
- Keep essential data on the server not workstation
- Know where your original licence disks are
- Understand your disaster recovery invocation procedure

Desktop Components Specification Templates

A. The LAN (Local Area Network)

This section should contain information to generally describe your LAN. If you need help to complete this template, please consult with your PC Support Team. It must contain the following information:

LAN name:	
Location address:	
Contact names/Telephone numbers: ⇒ LAN Administrator ⇒ Secondary contact ⇒ Business Contact	
Operating Company	

B. File Server(s)

This section should contain information generally describing each of your File Server(s). If you need help to complete this template, please consult with your PC Support Team. It must contain the following information:

	File Server 1	File Server 2
Type of server e.g. File, Print, Database or Communications		
Hardware make/model e.g. IBM PC Server 500		
Processor used e.g. P200		
Total memory (Mb)		
Total Disk capacity (Gb)		
Operating system e.g. Novell Netware 3.12/4.01, OS/2		
Any relevant Network Directory systems (NDS) information e.g. treename		
Volume or partition name and sizes (Mb)		
What name spacing is in use and on which volumes(s)		
Details of where to get the Licence for this server		
Level of software patches on this server		
Detail any SCSI card(s) or tape streamer ?		

C. Workstation Recovery Information

This section should contain information describing what is required on your workstations and the numbers required in a disaster recovery scenario. If you need help to complete this template, please consult with your PC Support Team. It must contain the following information:

	File Server 1	File Server 2
Hardware specification(s) e.g. make/model e.g. IBM 350 P75 memory (Mb) disk capacity (Gb)		
Number required of each hardware specification		
Operating System e.g. Windows 3,1, 3.11, 95		
Include any configuration information		
Note: Where possible, all software used on the workstations should be installable from the server. Where it isn't, show where the software is kept and how to get hold of it		
Which software packages, including version number, are required and where found		
Numbers required of each software package		

D. Printer Information

This section should contain information describing your printer requirements and the numbers required in a disaster recovery scenario. If you need help to complete this template, please consult with your PC Support Team. It must contain the following information:

Hardware specification e.g. make/model e.g. HP laserjet 4	
Any other non-standard features, additional memory, Postscript, dual-bin, etc.	
Numbers required of each hardware specification	

E. Other Hardware/Services Information

This section should contain information describing any additional hardware associated with your LAN and the numbers required in a disaster recovery scenario. If you need help to complete this template, please consult with your PC Support Team. It must contain the following information:

Hardware description e.g. modem/scanner	
Hardware specification e.g. make/model	
Software required	
How is the software obtained	
Describe the service	
How is the service obtained	

F. Invocation Procedures

Standard invocation procedure must exist for this LAN. If you need help to complete this template, please consult with your PC Support Team. In addition, the following must have been determined:

Invocation procedure: Telephone call to: Information required to be supplied e.g. LAN name, location, etc: Authorised Business Personnel who can request invocation service:	
Non standard invocation procedures: - other technical supporting teams - other third party suppliers - recovery sites	

G. Vital Records and Backup Information

This section should contain information describing the backups taken of your LAN. If you need help to complete this template, please consult with your PC Support Team. It must contain the following information:

Which server contains the backup hardware ?	
What type of hardware is used to take the backups (make/model) ?	
Which software is used (name/release/version) ?	
How can the passwords associated with the backups be obtained ?	
Where are the backup tapes kept ?	
Who or what procedure is used to take them to the offsite store ?	
What is the frequency of backup and does it depend on the day of the week, the week in the month and/or month in the year ?	
What other information is kept at the vital records store ? e.g. documentation, recovery procedures, timescales and priorities, business processes, etc. ?	
Detail information regarding the offsite store e.g. location address, passwords required, telephone numbers ?	
What is the retrieval procedure ?	
Who is authorised to retrieve the backups ?	

H. Recovery Site Information

This section should contain information describing the workarea recovery site. If you need help to complete this template, please consult with your PC Support Team. It must contain the following information as a minimum:

Name of recovery vendor/premises	
Recovery Site Address	
Recovery site locality information and map	
Any other relevant information	

I. Appendices

This section can contain any relevant information. If you need help to complete this template, please consult with your PC Support Team. A few suggestions may be:

Printed copy of NDS	
Prints of start-up/autoexec files	
Total contents list of offsite vital records store	
Details of acceptance tests to be run once recovery is complete	

When complete, this form should be discussed with Information Technology Services.

MIDRANGE SYSTEMS

RECOVERY PLANNING & TEMPLATES

Define all the software applications in use on the system

This list should contain all software applications that are in use on the system and should include infrequent usage products as well as everyday ones. The provision of version and licence number gives the component uniqueness to your environment.

Business Process or Function	Software Product	Version Number	Licence Number	Operating System ✓ or x	Bought in Software ✓ or x	Own written software ✓ or x	Linkage software to other products or services ✓ or x	Frequency of use D= daily W= weekly M= monthly etc.	Essential ✓ or x	Useful or nice to have ✓ or x

Define all the data files stored on the system

This list should contain all the data files that are in use in on the system and should include infrequent usage files well as everyday ones.

Business Process or Function:	Directory Or file name:	Essential ✓ or x	Useful or nice to have ✓ or x	Backup taken ✓ or x and frequency	Word Processing ✓ or x	Spread Sheet ✓ or x	Database ✓ or x	Other ✓ or x

Many or a number of applications on the midrange system can be deemed business critical if you have a tick in any of the boxes in the above two tables indicating essential.

The business critical midrange system applications must now be defined in more detail; only give details of what is essential to be available. These requirements will define the key elements of the system which is to be recovered as soon as possible after the disaster or incident. Non-essential, useful or nice to have applications or data can always be recovered at a later time.

Midrange Continuity

In answering the questions below, any response that falls into a shaded box may mean that the disaster recovery preparedness of your midrange system is not complete and may indicate that further preparations have to be considered.

		YES	NO
Acceptance Tests	Have you prepared a series of short comprehensive test scripts to run when the midrange system(s) is restored/recovered to check that it is functioning OK and all systems/transactions/data are available ?		▨
Acceptance Tests	Have you prepared a series of short comprehensive test scripts to run when the Midrange system(s) is restored/recovered to check that printers and any special connections are working ?		▨
Access Control	If any/all of your systems, applications, files, processes are password protected, could you foresee any situation where a critical password may not be available so hindering/preventing progress of the recovery ?	▨	
Access Control	If yes, do you keep a set of emergency passwords at the vital records store (provided it is secure enough) ?		▨
Backups	If you take your own backups, do you keep them at the vital records store or offsite ?		▨
Backups	Do you have a different backup routine depending on the day of the week, the week in the month and/or the month in the year ?		▨
Backups	Is the backup restore procedure documented ?		▨
Backups	Has a restore/recovery of the backups been undertaken to test that the backup procedure has been done correctly ?		▨
Backups	If so, did you encounter any problems ?		▨
Backups	Has a restore/recovery of the backups been tried to equipment different to that which you normally use ?		▨
Backups	If so, did you encounter any problems ?		▨

Backups	Are there any system requirements or defaults that must be in place prior to commencing the restore/recovery from backups ?	▨	
Configuration	Have you documented the minimum specification for the system ?		▨
Configuration	Are all/any system configurations detailed so that a competent technician could rebuild it ?		▨
Dependency	Does this system require any other software or hardware outside its normal environment to be available for it to function ?	▨	
Midrange including LAN	Have you completed the Midrange Templates and discussed your requirements with Information Technology Services Midrange DR providers team ?		▨
Hardware & Software	Do you have a complete list of all hardware and software installed on your system(s) ?		▨
Hardware & Software	Has this list of hardware and software been reviewed in the last six months ?		▨
Hardware & Software	If you need additional hardware and software to be obtained and installed at the recovery site, can it be achieved in the timescales required ?		▨
Hardware & Software	Do you require connectivity to other systems/services e.g. BACS ?	▨	
Hardware & Software	Is this connectivity requirement documented ?		▨
Hardware	Do you have any customised equipment that cannot be purchased/replaced off the shelf ?	▨	
Hardware	Have you considered the impact on your business if you do not have this customised equipment ?		▨
Invocation	Do you know and have documented the invocation procedure for midrange DR ?		▨
Recovery Time	Do you have a documented timetable for the order and timings that any recovery/restore will take ?		▨
Salvage	If the data on your hard-disk is unavailable, have you considered the implications of not being able to get access to it, either short or long term ?		▨
Security	Do your system(s) have any confidential or sensitive data or information on it that may require special considerations when running at another site ?	▨	

Software	Are you running any software that is not longer supported by the supplier and may therefore cause problems when installed in a different environment ?	▨	
Software licence	Is a new licence required for change of hard disk running environment ?	▨	
Technical Manuals & Documentation	Does the recovery centre have the technical manuals for the equipment installed and basic operating systems ?		▨
Technical Manuals & Documentation	Are all your system procedures documented and copies kept offsite or at the vital records store ?		▨

Responsibilities of Information Technology Services and the Business

Planning/recovery responsibility:	**Business**	**Midrange Administrator**	**IT Services**
Establish what of midrange system and applications is business critical	✓		
Identify hardware & software requirements etc.	✓		
Establish backup strategy	✓		
Establish recovery timetable and prioritise recovery of components	✓		
Backup of system, applications and data files	✓		
Recover operating system		✓	
Recover applications and data files			
Connect system to network, if required		✓	
Install/configure any additional connectivity hardware e.g. modems		✓	
Set up printer and produce test output to confirm recovery/connectivity		✓	
Negotiate disaster recovery contract with third-party			✓
Provide list of authorised business personnel who can request Midrange disaster recovery service	✓		
Invoke contract			✓
Co-ordinate recovery			✓
Document business process	✓		
Obtain hardware quote/contract for any hardware not met in third party contract			✓
Write business recovery plan	✓		
Write midrange disaster recovery plans		✓	

Preparing your Plan - Guidelines

The following may be used as a general template for preparing a Business Continuity Plan. However, some adjustments will inevitably be required in order to tailor the plan to the needs of your business. In addition, some activities may be performed concurrently.

Outline of Business Continuity Strategy

A brief outline **should** be included of the general approach adopted towards the provision of Business Continuity facilities.

Advise Emergency Services

Procedures **must** be defined for reacting to a crisis, ranging from alerting emergency services (police, fire service, ambulance, public utilities) to evacuating the building. If possible, aim for an orderly shutdown but staff safety **must** remain the highest priority.

Alert Internal Team

Procedures and priorities for contacting key individuals in the event of a disaster **must** be put in place. The roles and responsibilities of all major participants in the recovery process from a disaster **must** be clearly set out in advance to avoid duplication, conflicts of leadership and unassigned tasks. Responsibilities **should** be stated as a minimum for:

- liaison with emergency services;
- health and safety;
- security;
- staff well-being;
- liaison with suppliers;
- initiating and managing recovery;
- agreeing priorities;
- ad hoc decisions.

Please remember that some of the front line people may not be contactable, affected by the disaster or in a state of shock, so a mechanism is needed for calling in substitutes.

Assess Damage

Procedures are required for assessing the damage following an incident and securing the premises. Nominated persons **should** assess the degree of damage, the likely period of disruption to services, the severity of the business consequences and the possibility of continuing to operate without invoking contingency.

One of the early tasks **should** be to ensure that security is provided for the site to prevent unauthorised people from entering it and equipment, fixtures and fittings being removed without authority.

Escalate to Executive Management

Depending on the extent of the damage and its impact on the business, appropriate levels of management in the business **must** be notified before taking the decision to invoke contingency.

Decide Whether to Invoke Crisis Management

Once appropriate levels of management have been consulted and an authorised person has made a decision, there **must** be procedures for declaring the incident a disaster and invoking the plan.

Advice of Crisis Management

This involves procedures and priorities for contacting those individuals who are required to advise on the extent of the contingency arrangements to be invoked to deal with the particular disaster (e.g. salvage experts, loss adjusters). It may also be appropriate to give early warning to suppliers of essential goods and services that their assistance may be required.

Note that the Crisis Management Team (CMT) has responsibility for co-ordinating actions across the company following a major disaster.

Establish Command Centre

A Command Centre **should** be set up to manage the recovery. The location and telephone number(s) of the Command Centre **should** be detailed in the plan.

Call in Recovery Management Teams

Procedures and priorities **should** be set out for calling in those personnel required to carry out the recovery processes as defined in the Business Continuity Plan.

Commence Recovery Process

This is a specification of the procedures to be followed as part of the contingency arrangements. It **should** specify the following where relevant:

- initial physical locations for equipment and staff;
- other resources required (for example, telephones and photocopiers, fax machines);

All Business Continuity Planning processes **should** consider the worst case scenario. Where implementation of the contingency arrangements is phased, the plan **must** include details of any interim procedures before establishing the full contingency service.

If contingency involves operating from a different site, it **must** be checked that all required services and utilities can be made available by those responsible for that site. The plan **should** also consider the means by which a transfer to alternative permanent working arrangements will be achieved if the contingency service is only for a limited duration.

Where there are interdependencies with other plans (whether business or Information Technology related), steps **must** be taken to ensure that the proposed procedures are compatible.

General Advice

Procedures **should** be developed for contact with:

- All other staff in the unit affected by the disaster, advising them about the action required of them;

- 'Customers’ of the unit, whether internal or external, to advise, firstly, that the disaster has occurred and secondly of the likely impact on them;

- Press and media, who are seeking information on the disaster and may require formal statements. One person should be nominated to co-ordinate contact with the media.

An up-to-date copy of the plan **must** be held off-site from the building for which the plan is prepared. Copies of all other documentation necessary to support contingency running **must** also be held off-site and be accessible after a disaster. The back up documentation should be stored sufficiently far from the main site as not to be affected by the disaster.

Other Considerations

However good the planning process, not all consequences will have been considered. If a disaster occurs, the success of the recovery operation depends on the loyalty and goodwill of the staff. Managers must ensure that staff understand their tasks following a disaster and are given appropriate training. Even with training, staff will not be well versed in the procedures to be adopted.

A list of items for consideration when developing the contingency plan follows. It is not exhaustive but includes some of the less obvious items which companies who have suffered a disaster either found beneficial or wish they had included in their own contingency plans.

Staff-related issues

- Consider staff welfare (including facilities for them to contact their families).
- Arrange special transport for staff working at a new location or working extended/unsociable hours.
- Plan for emergency hotel accommodation and on-site refreshment facilities to be provided at short notice.
- Relax clothing rules because long hours are being worked or conditions may be dirty.
- Consider measures to avoid worker fatigue as staff work long hours out of dedication and loyalty e.g. shift working.
- Call in medical advisers to check staff for signs of trauma or delayed shock.
- Identify sources of replacements for staff incapacitated or lost as a result of the disaster.
- Consider special bonuses to staff who have made outstanding efforts.

Management Issues

- Increase security around the stricken area due to the higher risk of theft and looting.
- Ensure that suppliers of contingency services are sufficiently far away as not to be affected by the same incident.
- Provide public relations information and press briefings.

- Utilise professional assistance in loss adjustment and salvage in consultation with Group Risk Management.
- Supply mobile phones in case the PABX is not available.
- Identify contacts in Facilities to advise on emergency work, available space and building repairs.
- Talk to the emergency services while developing the plan to understand their plans and learn from their local knowledge.
- Collect photographic evidence of the damage before recovery commences for insurance or legal evidence purposes.

Procurement issues

- Nominate one individual to be responsible for ordering all new and replacement equipment to avoid duplication.
- Get an opinion on the possibilities of salvaging damaged equipment.
- Maintain contact names and phone numbers for key firms in the second-hand equipment market.

Where possible, order equipment on a sale-or-return basis and ascertain whether equipment can be rented rather than purchased.

All people who may need to access the information must know the location of the plan. Measures should be taken to protect the plan from unauthorised modification or destruction.

SECTION TWO:

CONTINGENCY PLANNING

CONTINGENCY PLANNING TEAM CHAIR – INITIAL TASKS

The following tasks give a suggested approach to the role in planning mode

1. Familiarise yourself with the Business Continuity Management Companion Guide

2. Prepare Emergency Response Procedures for your premises:

- Establish Emergency Co-ordinator,
- Ensure adequate coverage of Emergency Marshals and First Aiders throughout premises
- Write detailed procedures for all persons with an identified role
- Run training sessions for all persons
- Consider findings from premises Risk Analysis

3. Build Contingency Planning Support Team:

- Include members from security, maintenance, and engineering
- Prepare call lists including out-of-hours
- Train all members in their roles and responsibilities
-

4. Identify and set up Emergency Control Centres

- Locate suitable locations for both primary and secondary Emergency Control Centres
- Make formal arrangements for use of these locations with owner
- Ensure access is available 24 hrs/day and at short notice
- Prepare contents for Battle Boxes

5. Customise the Contingency Plan:

- Detail the people and resources needed
- Consider the responses to differing scenarios e.g. fire, flood, denial of access, bomb threat, chemical spillage, etc.
- Complete Yellow Pages

6. Test your plan and update procedures:

- Test emergency response procedures and contingency plan, initially table-top exercises moving up to full evacuation tests

- Analyse results from tests and update procedures and vital records as appropriate

- Consider holding Contingency Planning meetings at one of the designated Emergency Control Centre so that members gain familiarity with surroundings

PLANNING AND PREPARATION

Contingency Planning Team

This team has a chairperson and members; no maximum number but normally no more than five and is comprised of representatives of those residing in the building together with a representative from Facilities Management, where available.

It is the responsibility of the Contingency Planning Team chairperson to ensure that a Contingency Plan is written for the building and regularly reviewed and updated. This is a planning and preparation role.

At the time of a serious incident, the Contingency Planning Team meet as soon as possible and make a quick assessment of the situation as known. The following criteria may be used to decide if the incident requires the Crisis Management Team to convene and declare an incident.

- If the business at the building concerned may be critically disrupted for more than four hours of continuous working
- Any fatal injury occurring at the building
- In the event of a bomb threat or where a bomb is positively identified
- Where an extortion threat is made
- Any incident or event judged by the chairperson or deputy to be of such gravity for the Contingency Planning Team to meet to consider the incident

If the incident can not be handled by the local Contingency Planning Team, then the Contingency Planning Team will convene as the Crisis Management Team. At such time, they will/may be augmented by support from other parts of the business e.g. Risk Management and Security.

Initial Emergency Response Procedures

These are a vital set of procedures that are mandatory in all Group buildings. For a small office with just a few staff, they are likely to be simple and require less than a side of A4 paper. In larger buildings, these procedures are likely to be complex and involve many personnel.

However the size of the building is not critical; the key factor in initial incident response procedures is to provide building occupants (staff, visitors, contractors, public, etc.) with brief procedures on what to do if they:

- see smoke or fire
- find a suspect package
- receive a bomb threat telephone call
- see person(s) behaving suspiciously
- have to evacuate the building(s)
- observe any other incident or activity which causes concern

The procedures get more complex in larger buildings e.g. campus sites, as there are likely to be specialist personnel often concerned with the running of and services provided in the building i.e. maintenance engineers, facilities staff, security guards, etc. In these cases, the procedures will detail the responsibilities of building occupants and also the role of the specialist personnel.

Together, all the roles work towards providing building occupants with a safe environment and in the event of an incident or potential incident provide them with a safe exit from the building and minimising the impact of any incident.

Emergency Co-ordinator

Several roles exist in building initial emergency response procedures but the key role is that of the Emergency Co-ordinator.

Once the building has been evacuated and staff are located in the predetermined Assembly Area or other as appropriate, the Emergency Co-ordinator will notify the Contingency Planning Team chairperson by the quickest means of the situation as known. The Contingency Planning Team will convene at the appropriate Emergency Control Centre.

The Emergency Co-ordinator will appoint a representative to liaise with the Emergency Services at the scene of the incident. The Emergency Co-ordinator will also organise means of communication between the Assembly Area, the Contingency Planning Team at the Control Centre and the Incident site.

The Emergency Co-ordinator through the Chief Emergency Marshal and the Emergency Marshals has prime responsibility for the safe evacuation of the building(s) and the movement of staff etc. to the designated Assembly Area. Once in the Assembly Area, the Emergency Co-ordinator's responsibility is the:

- control and communication with staff etc. in that location
- provision of updates to the Contingency Planning Team
- control of personnel in and out of the Assembly Area
- liaison with the relevant Emergency Services, not otherwise catered for by the Contingency Planning Team
- welfare and safety of staff assembled within the designated Assembly Area

Personnel should not enter or leave the Assembly Area without notifying the Emergency Co-ordinator or his representative. Personnel in total may only be released from the Assembly Area by the Emergency Co-ordinator on instructions from the Contingency Planning Team.

If the Contingency Planning Team decide that staff should be sent home, then this must be advised to the Emergency Co-ordinator who will announce this decision to all those in the Assembly Area.

Chief Emergency Marshal/Emergency Marshals

Emergency Marshals also assist the safe evacuation of building occupants.

Every building should have a team of Emergency Marshals. In small buildings, this may be a minimum of two personnel increasing in numbers for larger sites, especially campus sites.

A Chief Emergency Marshal should be appointed to train and co-ordinate the activities of all other Emergency Marshals in the building(s) to ensure total coverage and consistency. Emergency Marshals must be trained in carrying out their duties if they are to be effective in the event of an incident. Emergency Marshals should be trained in the use of fire fighting equipment.

Where there are several Emergency Marshals to a floor or area, then one Emergency Marshal may carry the title of Senior Emergency Marshal and will co-ordinate the evacuation duties of the other Emergency Marshals on that floor or area.

The Chief Emergency Marshal, post an evacuation, will receive status reports from both Emergency Marshals and at a later stage Roll Call Marshals. Such reports will be collated by the Chief Emergency Marshal who will in turn pass such information to the Emergency Co-ordinator.

Emergency Marshals are responsible for checking and ensuring that all building occupants evacuate the building on hearing a continuous alarm signal. They are normally the last to leave a floor or area and check not only that all personnel have left by a safe route but that all toilets, closed but not locked rooms, conference and meeting rooms have been vacated as well. This check will also ensure that any disabled persons are evacuated safely as they may not hear or be aware of the fire alarms sounding.

Emergency Marshals should be provided and wear red tabards at the time of an evacuation or when undertaking an Emergency Marshal role.

Emergency Marshals should on completion of an evacuation report to the Chief Emergency Marshal the status of their area so that any unchecked areas of the building can be reported to the Emergency Co-ordinator who in turn will advise the Emergency Services when they arrive on site.

In a bomb threat or suspect package situation and under the direction of a Contingency Planning Team member, Emergency Marshals may be required to assist in moving personnel away from windows or to another area when it is not desirable to evacuate the building by the fire alarm system. They may also assist in searching stairwells, staircases and escape routes.

First Aiders

The number of qualified First Aiders in any building will be in accordance with the Approved Code of Practice as contained within the Health & Safety (First Aid Regulations 1981). First Aiders will be professionally trained by a recognised training body, approved by the Health & Safety Executive and recommended by the Health & Safety Manager.

Most buildings run on the principle of a Duty First Aider who will at the time of an evacuation take their first aid bag/box with them or collect one of the building first aid boxes and go to the Assembly Area or scene of incident, as appropriate. They should have a green tabard to wear in an evacuation so they can easily be identified.

Emergency Clothing

All Emergency Marshals and First Aiders should be provided with special clothing which clearly identifies them and their role i.e. Emergency Marshals should have red tabards with the words Emergency Marshal in white lettering on the rear and First Aiders should have green tabards in white lettering on the rear.

The colour and style of the clothing should not conflict with the Emergency Services.

Roll Call Marshal

At the Assembly Area some buildings will operate a Roll Call Marshal system. Their responsibility is to take a roll call of all persons present and to identify any persons not present in the Assembly Area. Their findings are reported to the Emergency Co-ordinator through the Chief Emergency Marshal.

Some larger buildings, mainly the campus sites, no longer carry out roll calls due to the large numbers of personnel on site and the fact that personnel generally move freely across the campus buildings. In such circumstances, it is imperative that all building occupants are evacuated by the Emergency Marshals. The Emergency Services will require confirmation that building(s) have been cleared. In such circumstances, departmental/section buddy checks must be carried out.

Assembly Areas

Two Assembly Areas need to be identified.

The first one, to be used in the event of a fire or other non-bomb evacuation, is an area of safety reasonably close to the building(s) but out of the immediate danger area. This may be a car park or public open space. This is known as the Primary Assembly Area.

The second one to be used in the event of a bomb evacuation should be a minimum of 800 to 1000 metres from the building. A resulting explosion can send debris and glass over a large area. In identifying a suitable second Assembly Area, known as the Secondary Assembly Area, consideration should be given to being out of line of sight from the explosive device, and ease of access from the building i.e. are there main roads to cross, busy traffic, and the need for support from the Police/Emergency Marshals to halt traffic if absolutely necessary and any other relevant considerations.

It is good practice to discuss the siting and use of all Assembly Areas with the Emergency Services (Police) so that they can advise on any known conflicts of site usage.

Staff Information Hot Line

Introduction

A telephone Hot Line facility should be set up as a planning and preparation role which will provide information to staff in the event of an incident which restricts the use of or access to any premises occupied by the Group. An example of the line established in the UK can be found in Section C1 of this Guide.

Usage

Staff may initially hear of an incident through the media, particularly when it occurs outside normal office hours; however, detailed information on the consequences for staff may not be given.

The Hot Line should provide these details by way of a recorded message which:

- We are disrupted/displaced but Computer Centre is undisturbed.
- will give information regarding the impact on company premises
- will be regularly updated
- will be available 24 hours a day
- will be for the use of company staff only.

An encapsulated card showing the number to call should provided to all staff. The card should be carried by the staff member or kept at home for use in an emergency.

Counselling

Introduction

Critical incident management naturally focuses on business continuity, premises, installations, facilities, computers, etc.. But what about the people ?

In recent years organisations have become more aware of the effects that critical incidents can have on their staff, repercussions that can last many years, affecting both the personal and working life of the people involved.

Organisations have been established to address the psychological needs of people in the workplace. Calling on years of experience of incidents such as armed raids, traffic accidents, murder and terrorist activities, they offer a programme of support and recovery to limit the psychological damage, bringing victims back to the pre-incident levels of energy and commitment.

In the aftermath of an incident, the expertise of a professional organisation used to handling the human issues, debriefing and counselling employees, can be very beneficial. Counsellors should not operate in a vacuum. They should be involved as a natural partner with those responsible for the controlled response to a crisis. Their benefit can best be felt when integrated into an organisation's total contingency plan.

If an organisation has developed a business recovery programme, time spent with a professional counsellor to define his/her role and contribution is invaluable.

Counsellors do not need to be on site the moment an incident occurs. They could just be in the way. In the immediate aftermath, victims are not available for counselling. Initially, they require medical attention, support and calming. It is in the following days that the counsellor's role will develop.

Humans are, by nature, resilient, adaptive and resourceful. A crisis often brings out the best in people. While the incident is taking place, humans function at very high levels of efficiency, composure and performance. It is after the adrenaline has stopped pumping and the crisis is either averted or over that help and support are needed from colleagues, family and friends.

Cause & Effects

The following short list highlights the effects on the victims of critical incidents.

Re-experience

This covers a wide range of reactions from the waking or dreaming recollection of the event to a sense of being once again overcome by the sights, sounds and smells of the original episode.

People with just a mild form of this reaction will recall the odour, a particular part of the vision or a peculiar taste in the mouth with startling clarity.

Free-floating

Free-floating emotions are unconnected or disproportionate to their cause. For instance, a person suddenly experiences panic in a car park although the event had nothing to do with a car park. A person could become extremely angry with someone or about something seemingly irrelevant.

It is very common for management to become a focus of anger on all sorts of issues whether or not they had anything to do with the incident itself.

Alternatively, people could feel unbearably guilty about an aspect of the event over which they had no control, even the simple fact of being away from the scene at the time.

Psychological reactions

These are more easily imagined: lack of sleep, loss of appetite, sudden outbursts, nightmares, nerves on edge, easily startled.

Avoidance reactions

This could be as simple as someone wanting to avoid the location of the event. More serious, however, is people trying to avoid all memory of it to the point of refusing to read newspapers, watch television or listen to the radio in case something should trigger a recollection. These extreme reactions need to be addressed early on before new patterns of behaviour become too deeply imbedded in the individual.

In general, staff should be given the opportunity to get together at the earliest opportunity either on or off site. The request to attend a debriefing session will achieve this and bring staff back to the featured location at an early date, whenever possible.

Alienation

This is a common phenomenon when those who have suffered a particularly disturbing experience feel that their view of life has been shattered or radically changed.

They have suddenly come up against the cheapness of life, especially of their own. They feel that they have brushed against death and are shocked by its meaninglessness, even perhaps its grotesqueness or the way it degrades its victims.
They consider that life will never be the same again.

"All it took was for his finger to twitch and I was dead" said one building society assistance who had held a gunman's eye for a few seconds. "I meant absolutely nothing to him".

Some victims believe they are marked for life, that they are now so different, so changed that others cannot possibly understand. The danger here is that individuals can become permanently locked within themselves.

Defusing: Briefing: Assessment & Counselling

Defusing is the process of bringing a situation under control. It starts immediately the crisis itself is over and the primary role belongs to management. Whatever else the victims may latter recall of the help they were given, people will always remember what attention was paid to them on the day by the management, by what a senior member of the organisation said and did. This dedicated role is tailor-made for managers, line or personnel, local, regional or national, whose natural reactions are to be supportive, attentive and relaxed.

At this point, people need someone who shows a genuine interest in them as individuals who will take a note of everything that everyone says. It should be someone who will not become defensive in the face of anger, someone who will take every suggestion seriously but not rushed into making promises. This is a time for listening. Reassurance and encouragement should be quietly expressed in what is done rather than what is said.

All this needs to be happening simultaneously with checking that people are physically cared for and comforted, that they have a safe place to go from work, that they have transport, that their questions have been logged. What has happened to others? Does the company's insurance policy cover torn clothing? Will this mean redundancies? Will they have to give evidence in court? Have the terrorists or raiders been caught?

A manager's final contribution as part of the defusing process is to encourage staff attend debriefing sessions which have been planned for the days following the crisis. In practice, most employees are anxious to return to work the next day if only out of a sense of loyalty to their colleagues and an eagerness to stay in touch. It is important that no-one is left out at this point and a structured debriefing session, properly led, will bring everyone involved into the process in a controlled manner.

Debriefing allows people to combine feelings with thought. Although a simple process, it needs skilful handling. It is essentially an invitation for people to talk about:

- what happened
- what their first thoughts were and
- which was the worst part

It is not designed to prompt strong emotions. It is more for people to be in touch with their feelings and combine these with their thoughts.

The greatest need people have when they have faced a life-threatening situation is to make sense of it, to digest and incorporate it within their own sense of reality. Usually, this is achieved by encouraging them to talk about it, time and time again in some cases. The greatest risk of psychological damage comes from denying this need. The greatest service anyone can do for a colleague, friend or family member who has been through what, for them, is a shocking and disturbing experience, is to give them the opportunity to talk about it and to keep on talking about it until they themselves tire of it.

Another common effect, where a number of individuals have together experienced a life-threatening situation, is the creation of a strong bond between them and a particular closeness and mutual support. It is helpful, particularly in the early days, to give them the opportunity to spend time with each other. Again, debriefing sessions will be helpful even more so when they include some individuals who are part of the normal team but were not present at the time of the incident and may themselves feel excluded.

There will, of course, always be individuals who feel safer or believe it more in keeping with their self-image to keep things to themselves and to swallow their reactions and keep quiet. This may be a constructive response and, in principle, their wishes should be respected. They should still, however, be invited to debriefing sessions which they may feel is a safer environment in which to open up.

One of the great benefits of debriefing is the opportunity to talk about what may be strange reactions but which are in fact shared by and understood by others. One of the main objectives is to normalise people's reactions and to reassure them that they are still in control.

A joint debriefing helps put together all the pieces of the jigsaw by combining everyone's contributions. Perceptions during a crisis can become distorted. An engine driver who sees a would-be suicide 800 metres ahead on the track is very likely to have a false sense of the timeframe. An employee watching a fire take hold may have a restricted recollection of the scene.

Similarly, people may develop entirely wrong perceptions, not only of what happened but of the behaviour and motivations of other individuals at the scene. They may also carry misconceptions of how others viewed their own behaviour.

Assessment and counselling provides professional help for those victims requiring further attention. While defusing can be done by certain people within the company and debriefing requires someone like a trained trauma counsellor. Assessment and counselling requires experienced, professional assistance.

More often than not, only a small proportion of individuals will need further counselling.

Ripple Effects

The ripple effects of an incident can travel surprisingly far and it is as well to be on the alert for those who are not the most obvious victims. Immediate family and work colleagues are an obvious category, as are the Emergency Services. Less obvious may be other members of staff who were not physically present but were somehow involved, like the despatch clerk who called out a fire crew and felt that she had sent one of the men to his death when he was caught by an unexpected blast or the young assistant manager of a small restaurant who was cashing up with his boss in the early hours of the morning and who managed to escape by sheer chance when the boss was subjected to horrendous violence.

It may be an employee who exchanged a shift with another who was hurt. It may be someone who had no real connection with the incident at all but for whom the event has triggered another crisis altogether.

Timescales

The first 24 hours belongs to the Emergency Services, the internal audit team if there has been a robbery, the rest of the Crisis Management Team and those particularly involved in the defusing process. Once the immediate aftermath has been cleared, however, debriefing should take place as soon as possible, for a variety of reasons. In particular to derive maximum benefit from positive group support and to interrupt potentially unhealthy reactions in individuals.

The ideal time for debriefing is somewhere between 48 and 72 hours following the event. After that, individual counselling for a very small minority may continue for a further four or five weeks.

Possibly some six to eight weeks after the crisis, a somewhat more relaxed follow-up in the same form as the first debriefing for as many people involved as possible, will help draw the threads together one more time and allow any remaining problems to be assessed, signalling a form of official end to the whole programme.

These sessions can be used to identify the small number of people who may start to show the effects of post traumatic stress disorder.

In practice, although at least 50 per cent of people will still say they have strong memories of most types of critical event even after three months, they will have been functioning at normal levels from a few days after it happened. Some will appear entirely unaffected throughout, most will be over the worst effects in a matter of days and the remainder inside two or three weeks.

Post traumatic stress disorder does not emerge until after several weeks and sometimes months of continuous symptomatology and is relatively rare, particularly when assessment and counselling have limited the worse damage and laid the foundations of a full recovery.

Media & Public Relations

A wide range of events could give rise to interest from the media. In broad terms press attention will be drawn by circumstances involving:

- We are disrupted/displaced but Computer Centre is undisturbed.
- loss of life or injuries to staff, visitors or tenants
- physical threat to staff etc. (including kidnap)
- fire, explosion, etc. preventing use of or access to the premises
- any major interruption to normal business use

In more serious cases, the Emergency Services will quickly take over and control the dissemination of information. In all cases whether we are working with the public services or on our own, our policy will be:

- to be as helpful to the media as possible, particularly where they can be useful in disseminating important information
- to pass on all media enquiries immediately to Corporate Affairs who will determine:
  - whether their on the spot attendance is required
  - who will be the company's spokespeople
  - the company's public statements
- to involve only those company departments or divisions directly interested in the event

"if you don't manage it, don't talk about it"

Emergency Control Centres

Introduction

At the time of an incident, it is likely that the building may be out of bounds so a meeting place for the Contingency Planning Team needs to be identified. This meeting place is known as the Emergency Control Centre (ECC).

Crisis Management Team

For small incidents or in the event of death or serious injury, the team may be able to meet within the building that they normally occupy but this should not be assumed.

The space required for an Emergency Control Centre is not large; a room for the Crisis Management Team to convene and from which to manage the incident. Ideally this could be in buildings where another building is close by i.e. on campus sites.

However, it may be necessary to acquire space/facilities provided from another company in the neighbourhood who, on a reciprocal basis, may be prepared to offer a room equipped with telephones, faxes, etc. Access to this facility should be available 24 hours a day and provide security and privacy. This is known as the **primary** Emergency Control Centre.

Certain incidents e.g. release of toxic fumes, bomb or gas leak may mean the identified Primary Emergency Control Centre is too close and inaccessible, so a secondary Emergency Control Centre should also be identified. This Secondary Emergency Control Centre may be several miles away and will need the same or similar facilities as the Primary Emergency Control Centre. Hotels may offer such facilities.

In both situations, written agreements on the arrangements and access with the owner of the identified building should be made.

All members of the Contingency Planning Team must know of these arrangements. It is a useful practice if some of the Contingency Planning Team meetings are held at the either of the Emergency Control Centres so that some familiarity of the locations and facilities is gained.

Battle Boxes

At the time of an evacuation, it is possible that only sketchy information may be available regarding the incident or the circumstances surrounding the incident. Once out of the building, return may not be possible for some considerable time, depending on the scale and cause of the evacuation.

For events other than a false alarm or minor incident, the Crisis Management Team should convene at the Emergency Control Centre. To assist them make an initial assessment of the situation and decide whether to invoke the Contingency Plan, they may need access to the Contingency Plan and other information that should be contained in a Battle Box.

This Battle Box may be a small portable box or briefcase. Two boxes should be maintained as a planning and preparation activity; one at the Primary Emergency Control Centre. However, if the Emergency Control Centre is at a location not owned by the company, it may not be possible for one to be kept at that site.

Each member of the Contingency Planning Team should have a copy of the Contingency Plan at home. If they are called to attend a Contingency Planning Team meeting, they should take their copy of the Plan to that meeting.

As a minimum, the contents of a Battle Box should be a copy of the Contingency Plan, a list of First Aiders and Emergency Marshals, personnel lists, a torch, notepad, mobile telephone, telephone card/chargecard and building layout plans.

CONTINGENCY PLANNING TEMPLATES

Contingency Planning Team Members

Name	Home Address	Telephone	Responsibility
		Office: Home: Mobile: Pager:	Chair
		Office: Home: Mobile: Pager:	Deputy Chair
		Office: Home: Mobile: Pager:	Emergency Co-ordinator
		Office: Home: Mobile: Pager:	Recovery Team Co-ordinator
		Office: Home: Mobile: Pager:	
		Office: Home: Mobile: Pager:	

Emergency Control Centres

Primary Emergency Control Centre for Contingency Planning Team

Location:	
Name of Company/Building:	
Contact name:	
Address:	
Telephone number:	
Fax number:	
Access – daytime:	
Access - out of hours:	
Distance from building (now incident site):	

Secondary Emergency Control Centre for Contingency Planning Team

Location:	
Name of Company/Building:	
Contact name:	
Address:	
Telephone number:	
Fax number:	
Access – daytime:	
Access - out of hours:	
Distance from building (now incident site):	

Crisis Management Team Members

Additional members may join the Contingency Planning Team to form the Crisis Management Team. They will be nominated by the Contingency Planning Team and their contact details should be recorded below as relevant. They may be drawn from Risk Management, Security, Property, Premises, Information Technology, Health & Safety, Human Resources, Media, etc..

Name	Office	Telephone	Responsibility
		Office: Home: Mobile: Pager:	
		Office: Home: Mobile: Pager:	
		Office: Home: Mobile: Pager:	
		Office: Home: Mobile: Pager:	

Pro-forma Agenda for Crisis Management Team

Suggested pro-forma agenda for first Crisis Management Team meeting below. It should be treated as checklist to identify the specific aspects of and responses to the incident under review. Not all agenda items will be relevant to every incident.

Pro-forma Agenda for Crisis Management Team first meeting**:**

1. **Establish scale of incident:**

   Loss of life

   Buildings partly/totally destroyed

   Major business functions stricken

   Data Centre/business systems lost

   Hostages taken

   Industrial action

   Major fraud perpetrated

2. **Assess impact(s) on business:**

   Operational status

   Customer service

   Competitive status

   Revenue streams

   Corporate liquidity

   Legal/regulatory requirements

   Public relations

3. **Decide on recovery strategy with business**

Activity Log

ACTIVITY LOG

Date: ________________

Time:	Activity:	Assigned to:	Review at:	Done ?	Comment

Log completed by: ______________________________________ Page __ of __

Expense Control

Department:____

Individual Completing Form: ______________________________________

Telephone Number: ___________________________ **Date:** _________________

Item Description:____

____

____

AMOUNT: Initial Estimate:______________________________________

Expense 'Incurred':__________________________________

Invoice Value:______________________________________

Does this item relate to a submission already made? Yes/No

Has this expenditure been authorised via the Crisis Management Team? Yes/No

Signed: ________________________ Team Leader/Manager

Name: ________________________ (please print)

For Risk Management Use Only:

Recovery Account Code: _________________ Unique Identifier: ______________

Notes: ____

____

Sheet______ of ______

CONTINGENCY PLANNING TASK LISTS

Contingency Planning Team

No	Activity	Comments
01	Convene Contingency Planning Team as soon as possible. Make initial assessment of incident and impact on business. If the scale of the incident cannot be handled by the local Contingency Planning Team, then convene the full Crisis Management Team. (Contingency Planning Team continue managing the incident locally). Decide which Emergency Control Centre to use if not already at one and advise those involved but not on site of the contact telephone numbers.	Use following criteria for assessment: • Is the business likely to be critically disrupted for more than four hours ? • Has there been a fatality ? • Is there a bomb threat or bomb found? • Has an extortion threat been made ? • Does the chairperson judge the situation to be of such gravity that the full Crisis Management Team should be convened ?
02	Appoint Contingency Planning Team chair who assumes responsibility for managing and co-ordinating the incident.	Ideally this should be the Contingency Planning Team chair but doesn't have to be.
03	Complete Incident Notification Pro-forma and start own incident log.	
04	Gather all information known regarding incident. Prepare summary of major findings.	Use reports from Emergency Co-ordinator, Emergency Services and others as available.
05	If dealing with a security alert or bomb threat situation which has been received via the telephone, check the detail of information received.	Check with the person who took the call: • What information did they get from the caller ? • When and where the alert will take place ? • Who was the caller ? • Anything unusual e.g. accent, background noise ?
06	Assess impact of incident on business. Decide if Recovery Plans need to be considered.	Contact Recovery Team Co-ordinator if not already part of team.

07	Appoint Contingency Planning Team Financial Administrator to take responsibility for all expenses and accounting. Liaise with Risk Management.	Compile list/summary of all expenditure. Risk Management telephone contact number: ( )
08	Assign task family task lists to other members of Contingency Planning Team or co-opt others as appropriate: • Facilities • Personnel Welfare • Casualties • Health & Safety • Media/Public Relations • Business Recovery Team Co-ordinator • Administration	Ensure that the person given the Media/Public Relations task list either: a) has previously had media training and received delegated authority or (b) knows that they must take direction from Corporate Affairs.
09	Compile message for the Staff Emergency Hot Line.	The first message can be issued by any Contingency Planning Team member but further messages must be authorised by the Contingency Planning Team chair. Hot Line telephone number:
10	Co-opt others as required.	Call on other resources to assist with any areas of work required.

Facilities Team

You have been asked by the Contingency Planning Team to carry out the following tasks in response to the incident which has recently occurred.

This task list is not conclusive; depending on the incident, other tasks may be required and some on the list not required. It is for guidance only.

Under no circumstances should contact be made with any media organisation. Please refer any requests for media contact to the assigned media spokesperson (see below).

Throughout the initial assessment period, please refer any questions or uncertainty to the Contingency Planning Team as they are responsible for managing and co-ordinating the incident.

No	Activity	Comments
01	Set up own incident log.	
02	Obtain name of media contact from Contingency Planning Team.	Do not have any discussions with the media - this is a sensitive and specialist area.
03	Make building plans available to the Emergency Services. Identify areas of sensitivity e.g. computer rooms, etc. Advise Emergency Services of isolation points for electricity, gas, water, etc.	Copies of building plans should be available in the Battle Boxes. If required, assist the Emergency Services in isolation of electricity, water or gas services.
04	Make area safe, cordon off with barriers, etc.	Black/yellow tape is very useful.
05	Keep Contingency Planning Team briefed.	
06	Do not allow any evidence to be moved or taken away. Use a camera or video to record evidence at scene of incident.	This should be done as soon as circumstances safely allow. The Police may request to see CCTV footage. Take copy of tape, to maintain own copy, before handing over.
07	Log all expenditure and submit log periodically to Contingency Planning Team Financial Administrator.	
08	When it is safe to re-enter the building, provide appropriate equipment e.g. hard hats, footwear, etc.	Re-entry into the building will initially only be authorised by the Emergency Co-ordinator and in turn the Contingency Planning Team chair or appointed representative.

Facilities Team (Continued)

09	Arrange for sufficient security guarding to: • protect site/perimeter • control access • prevent theft by opportunists • provide escort to search and recovery teams	Confirm arrangements for site perimeter security in liaison with Police. Boarding up of ground and first floors may be required if site has no perimeter fence. All personnel entering the building should be requested to visibly display their security pass. Use a different colour pass for staff and contractors.
10	Explain situation to arriving staff, visitors, customers or contractors.	
11	Make arrangements for collections and deliveries of mail.	Royal Mail may need to be asked to redirect mail to another address.
12	Advise suppliers of deliveries and make alternate arrangements.	Deliveries for the business units may need to be redirected to the Workarea Recovery Centres.
13	Depending on extent of damage, it may become necessary to serve notice of redundancy, freezing, suspending or terminating contracts of cleaners, caterers, etc.	Re-assignment to Workarea Recovery Centres may be appropriate.

Personnel Welfare

You have been asked by the Contingency Planning Team to carry out the following tasks in response to the incident which has recently occurred.

This task list is not conclusive; depending on the incident, other tasks may be required and some on the list not required. It is for guidance only.

Under no circumstances should any contact be made with any media organisation. Please refer any requests for media contact to the assigned media spokesperson (see below).

Throughout the initial assessment period, please refer any questions or uncertainty to the Contingency Planning Team as they are responsible for managing and co-ordinating the incident.

No	Activity	Comments
01	Set up own incident log.	
02	Obtain name of media contact from Contingency Planning Team.	Do not have any discussions with the media - this is a sensitive and specialist area.
03	Account for everyone - roll call or buddy check at Assembly Area. Update Emergency Co-ordinator with findings.	
04	Keep Contingency Planning Team briefed.	
05	Log all expenditure and submit log periodically to Contingency Planning Team Financial Administrator.	
06	Control movement of staff, visitors and contractors. Compile list of those who leave the Assembly Area.	Some may need to leave the Assembly Area while initial decisions are being made. Log all persons leaving and ask them to call the Staff Emergency Hot Line for an update.
07	Obtain update from Contingency Planning Team. If long outage, make arrangements for personnel to be sent home, moved to inside accommodation, etc. Arrange transport facilities.	Staff may have no money for public transport, fuel for cars, etc. due to possessions still being in the building. Locksmiths may be necessary to help with no keys for cars and home. See Yellow Pages for details of locksmith.
08	Contact all staff not known to be in the building at time of incident. Brief on situation and how further information will be made available.	

Casualties

You have been asked by the Contingency Planning Team to carry out the following tasks in response to the incident which has recently occurred.

This task list is not conclusive; depending on the incident, other tasks may be required and some on the list not required. It is for guidance only.

Under no circumstances should contact be made with any media organisation. Please refer any requests for media contact to the assigned media spokesperson (see below).

Throughout the initial assessment period, please refer any questions or uncertainty to the Contingency Planning Team as they are responsible for managing and co-ordinating the incident.

No	Activity	Comments
01	Set up own incident log.	
02	Obtain name of media contact from Contingency Planning Team.	Do not have any discussions with the media - this is a sensitive and specialist area.
03	Assemble First Aiders as resource to deal with casualties and as a possible resource for the Ambulance Service.	List of First Aiders in the Battle Boxes.
04	Compile list of casualties and fatalities, including hospitals used. The Emergency Co-ordinator may be able to provide more details.	Regularly update Contingency Planning Team with this list. **Only the Police can notify next-of-kin but they may request next-of-kin details from Human Resources Dept.** Liaise closely with the Emergency Services and Chief Incident Officer.
05	Log all expenditure and submit log periodically to Contingency Planning Team Financial Administrator.	
06	Send a representative to the Casualty Department of each hospital being used. Depending on the scale of the incident, the Emergency Services may set up a local Casualty Reception Centre for the initial assessment and minor treatment of casualties.	Where staff accompany casualties, etc. to hospital, details must be provided to the Emergency Co-ordinator at the earliest possible time.
07	Gather together any personal belongings of casualties; bag and label.	Casualty may have been taken to hospital from the street as well as from the buildings.

Casualties (Continued)

08	If given the OK from the Emergency Services, arrange interviews of the casualties and witnesses.	Liaise with Human Resources before carrying out.
09	Injured persons and their families may be pestered by the media for statements, stories, etc.	Liaise with Corporate Affairs as to how this should be dealt with.
10	Alert designated post trauma counselling agencies that their assistance may be required.	Counselling to be available to staff and their immediate relatives. Give early indication of number of casualties, witnesses, etc.

Health & Safety

You have been asked by the Contingency Planning Team to carry out the following tasks in response to the incident which has recently occurred.

This task list is not conclusive; depending on the incident, other tasks may be required and some on the list not required. It is for guidance only.

Under no circumstances should contact be made with any media organisation. Please refer any requests for media contact to the assigned media spokesperson (see below).

Throughout the initial assessment period, please refer any questions or uncertainty to the Contingency Planning Team as they are responsible for managing and co-ordinating the incident.

No	Activity	Comments
01	Set up own incident log.	
02	Obtain name of media contact from Contingency Planning Team.	Do not have any discussions with the media – this is a sensitive and specialist area.
03	Undertake appropriate notification to Local Authority in the case of injuries or fatalities.	Only the Police can notify Next-of-kin.
04	Depending on incident, consider if catering should be halted.	
05	Keep Contingency Planning Team briefed.	
06	Log all expenditure and submit log periodically to Contingency Planning Team Financial Administrator.	
07	Ensure entries are made in the building Accident Book, as appropriate.	All accidents and injuries to be recorded. Refer any general queries to the Health & Safety Manager .

Media & Public Relations

You have been asked by the Contingency Planning Team/Crisis Management Team to carry out the following tasks in response to the incident which has recently occurred.

This task list is not conclusive; depending on the incident, other tasks may be required and some on the list not required. It is for guidance only.

You are the only person on behalf of the business except members of Corporate Affairs who can issue a statement/briefing to any media organisation.

Throughout the initial assessment period, please refer any questions or uncertainty to the Contingency Planning Team as they are responsible for managing and co-ordinating the incident.

No	Activity	Comments
01	Set up own incident log.	
02	Contact Corporate Affairs for guidance on how, what and when to speak to any media organisation.	Log name of Corporate Affairs and contact telephone number.
03	Prepare a short, factual briefing statement for the media organisations e.g. radio, newspapers, television, etc. **If at all possible, agree content with Corporate Affairs before release to media.**	Where possible arrange a joint session with the Emergency Services. The Chief Incident Officer may co-ordinate statements and act as focal point in the early stages.
04	Keep Contingency Planning Team briefed.	
05	Log all expenditure and submit log periodically to Contingency Planning Team Financial Administrator.	
06	Prepare statement for main switchboard telephonists to give callers, whether staff or clients, an agreed script.	

Administration

You have been asked by the Contingency Planning Team to carry out the following tasks in response to the incident which has recently occurred.

This task list is not conclusive; depending on the incident, other tasks may be required and some on the list not required. It is for guidance only.

Under no circumstances should contact be made with any media organisation. Please refer any requests for media contact to the assigned media spokesperson (see below).

Please refer any questions or uncertainty to the Contingency Planning Team as they are responsible for managing and co-ordinating the incident.

No	Activity	Comments
01	Set up own incident log.	
02	Obtain name of media contact from Contingency Planning Team.	Do not have discussions with the media – this is a sensitive and specialist area.
03	Appoint runners to convey messages between Emergency Control Centre, Emergency Co-ordinator and Assembly Area.	Ensure that persons are available to act as messengers.
04	Equip Emergency Control Centre with office needs e.g. stationery, telephones, faxes, photocopier, etc.	
05	Get Battle Boxes to Emergency Control Centre if not already there.	
06	Ensure that the Contingency Planning Team have sufficient access and availability to food and drink.	It is very easy to forgo eating and taking sufficient rest periods.

Recovery Team Co-ordinator

You have been asked by the Contingency Planning Team to carry out the following tasks in response to the incident which has recently occurred.

This task list is not conclusive; depending on the incident, other tasks may be required and some on the list not required. It is for guidance only.

Under no circumstances should contact be made with any media organisation. Please refer any requests for media contact to the assigned media spokesperson (see below).

Throughout the initial assessment period, please refer any questions or uncertainty to the Contingency Planning Team as they are responsible for managing and co-ordinating the incident.

No	Activity	Comments
01	Set up own activity log.	
02	Obtain name of media contact from Contingency Planning Team.	Do not have any discussions with the media - this is a sensitive and specialist area.
03	As Recovery Team Co-ordinator, convene meeting at Business Recovery Emergency Control Centre of all business units affected by the incident to consider/invoke/put on standby any Business Recovery Plan(s).	

SECTION THREE

BUSINESS RECOVERY

RECOVERY MANAGEMENT TEAM CHAIR – INITIAL TASKS

The following tasks give a suggested approach to the role in planning mode

1. **Familiarise yourself with the Business Continuity Management Companion Guide**

2. **Determine Business Recovery objectives:**

- What functions/business processes need to be recovered and in what order
- When are they needed
- Identify any specialist or a one -off equipment for which no backup is/can be provided
- Use findings from the Business Impact Analysis

3. **Determine Information Technology Recovery Objectives**:

- What technology resources are required e.g. LANs, mainframe, desktop services, mid-range systems, communications services
- What other resources are required
- Include findings from business systems applications review

4. **Establish Workarea Recovery centre:**

- Determine where you can operate from
- Set up formal agreement for use, duration and costs of occupancy
- Ascertain invocation procedure and time before occupancy

5. **Write recovery plan:**

- Detail the people and resources needed to recover
- Prepare step-by-step procedures for all required functions of your department/function
- Complete Business Recovery Templates
- Complete Yellow Pages (as appropriate)

6. **Test your plan and update procedures:**

- Test recovery procedures including Information Technology, initially table-top exercises moving up to full test at workarea recovery centre
- Analyse results from tests and update procedures and vital records as appropriate

PLANNING AND PREPARATION

Emergency Control Centres

For the same reasons as the Contingency Planning Team, the Business Recovery Team need a predefined location at which to assemble and hold at least their first meeting. Depending on the size of the business, this may be at the same location as the Crisis Management Team, or at a separate site.

Therefore two Emergency Control Centres for the Business Recovery Team should be identified and made known to all members of the Business Recovery Team.

See section one of this guide for more detailed information on Emergency Control Centres, in relation to Crisis Management.

Alternate Site Options

Introduction

Various options exist in the consideration of alternate workarea recovery sites. In deciding which alternative site to consider/use, the alternate site must be capable of providing the business units with the necessary resources and be available within the required timeframe.

To be viable, the endorsed strategy must be maintainable, testable and executable at all times. The strategy must be sponsored and endorsed by senior management.

Alternative 1 - Commercial Workarea Facility

A commercial facility provides an environment where critical functions could immediately move to a pre-determined and configured workarea which is complete with desk, chair, telephone, fax and LAN accessible PC. The ability to link into voice circuits (routed to the same facility within hours) would provide functions with basic tools to communicate with customers, support and other company personnel.

Alternative 2 - Acquire Rented/Leased Commercial Space

Commercial space can be rented in surrounding areas over time. There would be additional costs incurred for renovation, upgrade, configuration and moving costs. Local facilities (hotels and conference centre) offer a variety of services and office tools such as telephones, office equipment and furniture rental for additional fees.

Alternative 3 - Relocate to other company locations

Should critical business functions be displaced at any location, plans can be developed to have technology access provided from another company location. Physical relocation of resources and off site records can also be pre-defined to facilitate a staged transition to other locations.

There may be a requirement for relocated business functions to work in shifts.

Alternative 4 - Reciprocal Facility

Reciprocal agreements to provide backup workarea and/or processing capability on a best-effort basis may be either internal or external. Either way, they are probably the least effect expensive method of alternate site provision. They are also the least effective for several reasons:

1. appropriate physical space requirements, configured workarea and voice access would have to be available for immediate occupation and regular testing
2. logistics and performance issues would have to be defined and solutions implemented that are mutually agreeable
3. these arrangements necessitate co-ordinated (both partners) technology changes (hardware/software/capacity) and frequent testing of technical plans to validate changed environments
4. telecommunications connectivity requirements would have to be pre-defined to facilitate access to voice and data from the reciprocal location to resident functions at other Company locations.

Alternative 5 - Do nothing: Live with the Risks

This is not a viable alternative due to the potential operational and/or financial impacts.

There would be significant impacts to customer service.

RECOVERY MANAGEMENT TEMPLATES

Recovery Team Co-ordinator

Role	Name	Telephone
Recovery Team Co-ordinator		Office: Home: Mobile: Pager:
Alternate Recovery Team Co-ordinator		Office: Home: Mobile: Pager:

Business Recovery Team

Name	Home Town	Telephone	Role & Responsibility
		Home: Office: Mobile: Pager:	
		Home: Office: Mobile: Pager:	
		Home: Office: Mobile: Pager:	

Recovery Management Team Members

Name	Home Address	Telephone	Responsibility
		Office: Home: Mobile: Pager:	Chair
		Office: Home: Mobile: Pager:	Deputy Chair
		Office: Home: Mobile: Pager:	
		Office: Home: Mobile: Pager:	
		Office: Home: Mobile: Pager:	
		Office: Home: Mobile: Pager:	

Primary Control Centre for Recovery Management Team

Location:	
Name of Company/Building:	
Contact name:	
Address:	
Telephone number:	
Fax number:	
Access – daytime:	
Access – out of hours:	
Distance from building (now incident site):	

Secondary Control Centre for Recovery Management Team

Location:	
Name of Company/Building:	
Contact name:	
Address:	
Telephone number:	
Fax number:	
Access – daytime:	
Access – out of hours:	

Key Tasks

Process	Sub-process	Priority	Frequency	IT/COMMS ?

Staff Contact Numbers

Name	Home Town	Telephone	Call Order	Business Responsibility

Vital Records Inventory

Description of Vital Record	Medium e.g. paper, floppy disk, backup tape, etc.	Location

Key Bodies, Suppliers & Clients

KEY BODIES	NAME	CONTACT NUMBERS

KEY SUPPLIERS	NAME	CONTACT NUMBERS

KEY CLIENTS	NAME	CONTACT NUMBERS

Resource Requirements

(Requirements detailed over BUSINESS DAYS)

Furniture:

Item/Time (days)	**1**	**3**	**5**	**10**	**15**	**20**	**25**	**30**	**>30**
Tables (Desk sets)									
Tables (Workspace)									
Fireproof cabinets									
Filing Cabinets									
Book Cases									
Filing Cupboards									

Office Equipment:

Item/Time (days)	**1**	**3**	**5**	**10**	**15**	**20**	**25**	**30**	**>30**
Calculators	**15**								
Copiers (Access to)									
Copiers (Dedicated)									
Fax									
Microfiche Viewers									
Microfiche Printers									
Microfilm Printers									
Typewriters									
Mainframe Terminals									
Mainframe Printers									

Hardware & Software:

Item/Time (days)	1	3	5	10	15	20	25	30	>30

Special Requirements:
(In addition to Standard Office stationery as supplied by Administration)

Item	Quantity/Comments

Notes*:*

Workarea Recovery Centre

Location:	
Provider:	
Address:	
Telephone number:	
Fax number:	
Contact:	
Access daytime:	
Access out-of-hours:	
Other information:	

Activity Log

ACTIVITY LOG

Date: ________________

Time:	Activity:	Assigned to:	Review at:	Done ?	Comment

Log completed by: ______________________________________ Page __ of __

N.B. Third party specialist providers of Workarea Recovery Centres will normally detail the invocation procedure in the Contract; this may name certain personnel within the Company who are authorised to invoke the service.

Status Report Log

Department:	
Team Leader:	
Alternate:	

Author: ______________________ **Date/Time:** ______________________

Subject:

____

____

Status: **(Findings/Recommendations/Observations)**

____

____

____

____

____

____

____

____

____

____

Sheet _______ of _____

Expense Control

Department:______________________________

Individual Completing Form: ______________________________

Telephone Number: ____________________ **Date:** ____________

Item Description:______________________________

____

____

AMOUNT: Initial Estimate:______________________________

Expense 'Incurred':______________________________

Invoice Value:______________________________

Does this item relate to a submission already made? Yes/No

Has this expenditure been authorised via the Crisis Management Team? Yes/No

Signed: ____________________ Team Leader/Manager

Name: ____________________ (please print)

For Risk Management Use Only:

Recovery Account Code: ____________ Unique Identifier: ____________

Notes: ______________________________

____

Sheet______ of ______

RECOVERY MANAGEMENT TASK LISTS

Business Recovery Team

No	Activity	Comments
01	Convene Recovery Management Team.	
02	Set up own activity log.	
03	From information available from the Crisis Management Team and others, ascertain the potential/actual impact on the business(es) and agree action plans.	
04	Decide if Business Recovery Plans are to be invoked/put on standby and which Workarea Recovery Centres are to be used.	
05	Set up individual business unit teams.	
06	Assign task lists for Insurance and Salvage/Asset Protection.	
07	Nominate a Workarea Recovery Centre Co-ordinator to manage and co-ordinate the provision of services and facilities at the recovery centre(s).	Depending on the number of business units affected and individual arrangements made, there may be one or more Workarea Recovery Centres required. These may be in different parts of the country, another building or a third party provider.
08	Log all expenditure and submit log periodically to Business Recovery Team Financial Administrator.	

Individual Business Unit Team

No	Activity	Comments
01	Assemble individual Business Recovery Team(s).	Have a meeting with the key members of your department. Co-ordinate transport needs with the Workarea Recovery Centre Administration. Review staff needs and hold a kick-off meeting to schedule the tasks which follow.
02	Confirm Workarea Recovery Centre requirements.	Confirm with the Workarea Recovery Centre Co-ordinator that the pre-determined facilities for your department at the Workarea Recovery Centre are in place. This should be a case of confirming your Resource Requirements. Flag any items no longer required. You might be able to request additional facilities at this time. Prepare an inventory containing information regarding the facilities requirements of your department.
03	Assign retrieval of vital records task.	
04	If you have any LANs, Desktops or Mid-range systems that need recovering, contact Information Technology for assistance.	IT will arrange for third-party data recovery contracts to be invoked and provide technical co-ordination roles.
05	Be advised of when your Workarea Recovery Centre can be occupied by your team.	You will be notified when the Workarea Recovery Centre is ready for occupation by the Workarea Recovery Centre Co-ordinator. No team will be allowed to relocate without the approval of the Crisis Management Team.

06	Verify new Workarea.	Check that the office facilities with which you have been provided agree with those requested and/or pre-arranged. In particular: • Check telephones work as expected and have the correct extensions allocated • Check special stationery is available • Any other requirements
07	Organise the Department.	Organise the Workarea so that restoration and resumption of the Key Tasks can commence in an orderly way.
08	Co-ordinate replacement assets.	Co-ordinate furniture/equipment deliveries to the Workarea Recovery Centre with the Workarea Recovery Centre Team. Arrange for the delivery of any replacement items of equipment or furniture to the Workarea Recovery Centres through the Workarea Recovery Centre Team.
09	Restore backups.	IT will recover all LAN servers and provide technical assistance for the provisions of Information Technology services. Advise the Recovery Management Team of any problems associated with the recovery of back-up information.
10	Obtain replacement PC equipment.	Advise Recovery Management Team of the need to obtain essential emergency replacement PC hardware or software to provide recovery that is not provided by the DR contract.
11	Confirm stationery and office supplies requirements.	Review stationery and office supplies requirements and forward replacement requests to Workarea Recovery Centre Administration.

12	Notify important contacts.	Confirm with the Recovery Management Team who has been notified of the situation in broad terms at a high level. Contact: • non-critical suppliers • regulatory authorities • key clients, agents, services • staff at other sites who are dealt with on a regular basis to perform the Key Tasks. Reassure that they will soon be dealt with as normally as possible and give some indication as to when this will be. Report to the Recovery Management Team if it is felt that any important contacts have not been informed of the situation at a high enough level.
13	Check status of mainframe, mid-range LAN, WAN, etc. and communication links, as appropriate.	Once informed that computer services are available, have the team test that these have been properly restored, in particular: • the applications work as expect. • the data appears to be correct at the point in time to which it should have been recovered. • printers and any special connections work normally. • check the output is as expected e.g. from overnight runs for the days missed since the incident is delivered and appears to be correct. Establish status and availability of telecommunications links, both voice and data.
14	Confirm stationery and office supplies requirements.	Review stationery and office supplies requirements and forward replacement requests to Workarea Recovery Centre Administration.

With the Workarea Recovery Centre established, begin the restoration and resumption of business functions.

No	Activity	Comments
15	Perform Key Tasks.	The service the team should provide is limited to the Key Tasks as defined, unless the Crisis Management Team or Divisional Head indicates otherwise. Prioritise these tasks and arrange for their completion on as normal a basis as possible.
16	Assess business impact.	Review any considerations which are/may affect the recovery of the Key Tasks e.g. • are any special reports required from IT in addition to those which would normally be produced? • is there a need for extra staff to help deal with a backlog or rush of client queries? Discuss any special needs with the Recovery Management Team.
17	Attempt to restore work-in-progress.	Assemble and prioritise any work in progress that has been recovered from the incident site. Telephone key contacts to obtain confirmation and supporting information.
18	Sort incoming mail.	Prioritise the mail backlog and establish suitable procedures to receive new mail. If the mail does not fall in to the Key Tasks then file away. File work safely away in date sequence to be dealt with when the situation returns to normal. If the Mainframe, Mid-Range, LAN or WAN service has not yet been restored, sort mail into that which can be dealt with manually and that which requires the main-frame. If the delay will significantly affect service levels, acknowledge the issuer of the correspondence.
19	Deal with manual work.	Carry out any work that does not require technology services.

Vital Records

No	Activity	Comments
01	Retrieve off site materials.	Designated Recovery Management Team members with appropriate security access should retrieve materials which have been stored off-site.
02	Prevent further damage to media.	If important papers, floppy disks and/or essential documentation have been damaged, take precautions to ensure that further damage does not occur when removing these vital records.
03	Salvage vital records.	If allowed to do so, retrieve as much work-in-progress and other important material from the incident site. The Emergency Services may let a representative of your team on-site if the building is safe.

Insurance

You have been asked to carry out the following tasks in response to the incident which has recently occurred.

This task list is not conclusive; depending on the incident, other tasks may be required and some on the list not required. It is for guidance only.

Under no circumstances should contact be made with any media organisation. Please refer any requests for media contact to the Crisis Management Team.

Please refer any questions or uncertainty to the Crisis Management Team as they are responsible for managing and co-ordinating the incident.

No	Activity	Comments
01	Set up own activity log.	
02	Log all expenditure and submit log periodically to Financial Administrator.	
03	Liaise with Risk Management for all activity regarding: • Property • Insurers • Legal	
04	Keep Business Recovery Team briefed.	
05	Assist in the completion of any insurance claim.	
06	Be aware that staff or others in the building at the time of the incident may incur personal losses.	These may not be insured through their own policies.
07	If a salvage area has been set up, work with the team there to report all salvaged assets.	

Salvage/Asset Protection

You have been asked to carryout the following tasks in response to the incident which has recently occurred.

This task list is not conclusive; depending on the incident, other tasks may be required and some on the list not required. It is for guidance only.

Under no circumstances should contact be made with any media organisation. Please refer any requests for media contact to the Crisis Management Team.

Please refer any questions or uncertainty to the Contingency Planning Team as they are responsible for managing and co-ordinating the incident.

No	Activity	Comments
01	Set up own incident log.	
02	Log all expenditure and submit log periodically to Crisis Management Team Financial Administrator.	
03	Locate an area of suitable size e.g. spare office, warehouse, etc. to which everything removed from building can initially be taken for assessment and checking.	This should be reasonably close to the incident site but outside any cordoned off area, be secure and provide adequate fire protection.
04	For ease of identification when assets are removed, colour code incident building into areas by floor, phase or logical grouping. Use same coding at receiving salvage area so that when assets are received there they can be placed into the same area.	For example, assets removed from second floor should be placed in receiving area designated as second floor.
05	Set aside an area within the receiving salvage area for the receiving of salvaged papers and items which may have been blown from the building and retrieved from the street or surrounding area.	
06	Obtain full asset register listing from the affected business functions of all assets normally in their part of the building.	
07	Set up procedure to log the removal of all assets from incident building to receiving salvage area. As assets are removed, security should check that removal of assets is authorised, by whom and where they are being taken and signed out.	Note: pedestal desks should not be locked but taped securely with warehouse type tape as there is a tendency for keys to become separated. Do not remove contents.

08	Priority should be given to the removal of all personal belongings from the incident building e.g. handbags, coats, wallets, keys, etc. Ensure all such items removed are bagged in clear plastic bags and have a sticker on them warning that they may be contaminated, contain glass pieces, etc. (depending on incident).	Priority salvage should be for staff related assets and business critical. Liaise with Risk Management for Loss Adjuster contact.
09	Keep Recovery Management Team briefed.	
10	Arrange for any vehicles within the building perimeter to be moved to a designated motor dealership or agent.	Vehicles may be part of company fleet or employee owned.
11	Arrange for all equipment to be checked by a specialist company for possible contamination by carbon deposits.	This includes all electronic equipment and PC medium e.g. CD-ROM's, PC floppy disks. No unchecked equipment or medium must be taken for use at Workarea Recovery Centres without being certified as checked and OK to use.

Consideration for Equipment Damage following Explosion

1. Initial shock wave damage to silicon, glass components and enclosed devices is not always apparent. May look outwardly undamaged.
2. Risk of implosion from VDUs requires careful handling.
3. All identified key equipment to be cocooned to prevent further deterioration.
4. Keyboards may not be cost-effective to salvage.
5. Dumb terminals and VDUs with damage to casings or scratched screens may not be worth salvaging.
6. All systems units to be salvaged with attempted recovery of data
7. Low expectation of equipment and re-use
8. Catalogue all systems units by tag number, processor chip, memory and size of hard disk to assist in claim
9. Any salvage floppy disks to be expertly copied to new disk before use to prevent contamination and damage

Status Reporting

No	Activity	Comments
01	Meet with your Team Members to evaluate status.	Review outstanding issues and/or unresolved problems.
02	Report status to Recovery Management Team.	Report status of your department's business recovery to the Business Recovery Team.

Workarea Recovery Centre Co-ordinator

No	Activity	Comments
01	The Recovery Management Team will advise which Workarea Centre(s) are to be used. There may be one or more different centre(s) being used.	Liaise with Recovery Management Team for their **Critical Business Services, Workarea Recovery Centre(s) and timescales**.
02	Set up own activity log.	
03	Contact the provider of the Workarea Recovery Centre(s) and put on standby or invoke use of centre, depending on whether final assessment of incident and impact on business has been made.	The Workarea Recovery Centres may be within existing buildings or supplied by a third party
04	Assign task lists to others as appropriate for activity in preparing the facilities and services at the Workarea Recovery Centre(s): • Personnel Welfare • Health & Safety	
05	Log all expenses.	
06	Co-opt others as required.	Call on other resources to assist with any areas of work required.
07	Ascertain from the business unit(s) numbers of staff expected to move to the Workarea Recovery Centres and at what times.	
08	Liaise with the providers of the Workarea Recovery Centres to ensure all predefined equipment and furniture is in place as per contract.	
09	Liaise with the Workarea Recovery Centre facilities personnel regarding: • the level of security provided for both staff and building • the provision of office cleaning services including the removal of rubbish and confidential waste.	Establish procedure for identification and access of staff both daytime and out-of-hours.
10	Ensure minimum number of photocopiers are operational and check out arrangements for supplies of paper, toner, etc. including maintenance and breakdown.	

11	Set up stationery cupboard supplies for the normal usage items and make arrangements for ordering non-standard items.	May need to consider setting up secure area/safe, etc. for items such as blank cheques, etc. and the provision of suitable access controls.
12	Set up Post Room facility to mirror as closely as possible messenger service previously provided.	Consider both internal and external mail handling.
13	Prepare welcome booklet for all arriving staff giving details of health and safety provision, emergency procedures, first aid, post and messenger services, general administration, etc.	Post welcome and direction signs to Workareas at reception.
14	Set up shredder(s) or means of securely holding confidential waste paper until removal.	
15	In conjunction with Workarea Recovery Centre facilities personnel, arrange for an evacuation test using fire alarm system within one week of staff occupying the building.	
16	Designate an area for the receiving of records, disks, equipment, etc. either from vital records or salvaged from the incident site via the salvage location, before allowing it to pass out to the relevant business unit.	Log all items received.
17	Notify suppliers of known regular deliveries of new site and details.	Existing regular orders may need to be amended.

Personnel Welfare

You have been asked to carryout the following tasks at the Workarea Recovery Centres in response to the incident which has recently occurred .

This task list is not conclusive; depending on the incident, other tasks may be required and some on the list not required. They are designed to open up communication between the incident site, the business unit(s) displaced by the incident and the Workarea Recovery Centre. It is for guidance only.

Under no circumstances should contact be made with any media organisation. Please refer any requests for media contact to the Crisis Management Team

Throughout the initial assessment period, please refer any questions or uncertainty to the Crisis Management Team as they are responsible for managing and co-ordinating the incident.

No	Activity	Comments
01	Set up own incident log covering actions taken, tasks delegated and decisions made.	Where tasks are delegated, include review time.
02	Log all expenditure and submit log periodically to the Workarea Recovery Team Financial Administrator.	The Administrator can provide expense codes to be used.
03	Establish from the business unit(s) which Workarea Recovery Centres are being used and numbers of staff expecting to be at the new locations and in what time scales.	
04	Liaise with pre-defined transport providers to set up arrangements for transporting staff to new locations.	Consider pickup points, frequency of service, opportunity for park and ride, out-of-hours working, use of public transport etc. Some staff will not have access to public transport and either currently walk or use public transport to work.
05	Avoid bringing in too many staff on site at the same time in the initial occupancy period at the Workarea Recovery Centres.	Only bring people in who can be gainfully employed. Ideally they should be phased in by department or team. This allows some settling in before the next team arrives.
06	Oversee working hours expected of staff to ensure that adequate rest periods are taken or enforced.	
07	Provide a separate area where debriefing and counselling can take place in private.	This may be away from site e.g. a hotel.

08	Confirm provision for catering, both drinks vending and meals and what is/can be provided on site/offsite for daytime and out-of-hours working.	Consider drinks vending machines on free vend to help staff settle in.
09	Arrange local hotel accommodation for those staff and visitors who may need it.	
10	Agree with Personnel Departments criteria and payment calculations for staff who relocate in terms of travelling costs, overtime, etc.	
11	Check personnel records to ensure all employee information is up-to-date including home telephone numbers.	
12	Prepare and provide daily briefing progress update to staff not working at Workarea Recovery Centre but asked to either work at home or just stay at home.	Use Staff Incident Hot Line facility - co-ordinate through Crisis Management Team. Helps to keep those at home feel that they are not forgotten.

Health & Safety

You have been asked to carryout the following tasks at the Workarea Recovery Centres in response to the incident which has recently occurred.

This task list is not conclusive; depending on the incident, other tasks may be required and some on the list not required. They are designed to open up communication between the incident site, the business unit(s) displaced by the incident and the Workarea Recovery Centre. It is for guidance only.

Under no circumstances should contact be made with any media organisation. Please refer any requests for media contact to the Crisis Management Team

Throughout the initial assessment period, please refer any questions or uncertainty to the Crisis Management Team as they are responsible for managing and co-ordinating the incident.

No	Activity	Comments
01	Set up own activity log covering actions taken, tasks delegated and decisions made.	Where tasks are delegated, include review time.
02	Do not have any discussions with the media - this is a sensitive and specialist area.	Refer any approaches to Crisis Management Team.
03	Establish the maximum number of persons that can be present on site as stipulated on the Fire Certificate.	Ensure this figure is not exceeded.
04	Check that the premises have the minimum and correct requirements for fire signs, extinguishers, blankets, etc.	
05	Log all expenditure.	
06	Establish First Aid provision if First Aid facilities are not provided.	First Aid may be provided by on site security team or it may be necessary to set-up first aid boxes and a First Aider roster.
07	Issue DSE assessment to all personnel using workstations.	Provide remedial equipment e.g. footrests, wrists rests, copy holders, etc. where identified.
08	Locate Accident Book.	
09	Consider whether a COSHH assessment needs to be undertaken.	There should already be one in the building as a whole unless it has been an unoccupied building.

10	Despite the attractiveness, do not allow staff to bring in any portable electrical equipment from home UNLESS it can be tested by a qualified electrician for Portable Appliance Testing (this should only be used for the minimum period only).	Ask to see Portable Appliance Testing logs for all equipment provided at the Workarea Recovery Centres.
11	Appoint a Health and Safety representative.	
12	Prepare emergency evacuation procedures for all building occupants and carry out evacuation test using fire alarm system within one week of staff occupying building.	
13	Set up enough Emergency Marshals to cover all areas of the Workarea Recovery Centres occupied by staff.	Briefing session with new Emergency Marshals could help them become familiar with the layout and escape routes of the newly occupied building.

Desktop Components Specification Templates

The LAN (Local Area Network)

This section should contain information to generally describe your LAN. If you need help to complete this template, please consult with your PC Support Team. It must contain the following information:

LAN name:	
Location address:	
Contact names/Telephone numbers: ⇒ LAN Administrator ⇒ Secondary Contact ⇒ Business Contact	
Operating Company	

File Server(s)

This section should contain information generally describing each of your File Server(s). If you need help to complete this template, please consult with your PC Support Team. It must contain the following information:

	File Server 1	File Server 2
Type of server e.g. File, Print, Database or Communications		
Hardware make/model e.g. IBM PC Server 500		
Processor used e.g. P200		
Total memory (Mb)		
Total Disk capacity (Gb)		
Operating system e.g. Novell Netware 3.12/4.01, OS/2		
Any relevant Network Directory systems (NDS) information e.g. treename		
Volume or partition name and sizes (Mb)		
What name spacing is in use and on which volumes(s)		
Details of where to get the Licence for this server		
Level of software patches on this server		
Detail any SCSI card(s) or tape streamer ?		

Workstation Recovery Information

This section should contain information describing what is required on your workstations and the numbers required in a disaster recovery scenario. If you need help to complete this template, please consult with your PC Support Team. It must contain the following information:

	File Server 1	File Server 2
Hardware specification(s) e.g. make/model e.g. IBM 350 P75 memory (Mb) disk capacity (Gb)		
Number required of each hardware specification		
Operating System e.g. Windows 3,1, 3.11, 95		
Include any configuration information		
Note: Where possible, all software used on the workstations should be installable from the server. Where it isn't, show where the software is kept and how to get hold of it		
Which software packages, including version number, are required and where found		
Numbers required of each software package		

Printer Information

This section should contain information describing your printer requirements and the numbers required in a disaster recovery scenario. If you need help to complete this template, please consult with your PC Support Team. It must contain the following information:

Hardware specification e.g. make/model e.g. HP laserjet 4	
Any other non-standard features, additional memory, Postscript, dual-bin, etc.	
Numbers required of each hardware specification	

Other Hardware/Services Information

This section should contain information describing any additional hardware associated with your LAN and the numbers required in a disaster recovery scenario. If you need help to complete this template, please consult with your PC Support Team. It must contain the following information:

Hardware description e.g. modem/scanner	
Hardware specification e.g. make/model	
Software required	
How is the software obtained	
Describe the service	
How is the service obtained	

Invocation Procedures

Standard invocation procedure must exist for this LAN. If you need help to complete this template, please consult with your PC Support Team. In addition, the following must have been determined:

Invocation procedure: Telephone call to: Information required to be supplied e.g. LAN name, location, etc: Authorised Business Personnel who can request invocation service:	
Non standard invocation procedures: - other technical supporting teams - other third party suppliers - recovery sites	

Vital Records and Backup Information

This section should contain information describing the backups taken of your LAN. If you need help to complete this template, please consult with your PC Support Team. It must contain the following information:

Which server contains the backup hardware ?	
What type of hardware is used to take the backups (make/model) ?	
Which software is used (name/release/version) ?	
How can the passwords associated with the backups be obtained ?	
Where are the backup tapes kept ?	
Who or what procedure is used to take them to the offsite store ?	
What is the frequency of backup and does it depend on the day of the week, the week in the month and/or month in the year ?	
What other information is kept at the vital records store ? e.g. documentation, recovery procedures, timescales and priorities, business processes, etc. ?	
Detail information regarding the offsite store e.g. location address, passwords required, telephone numbers ?	
What is the retrieval procedure ?	
Who is authorised to retrieve the backups ?	

Recovery Site Information

This section should contain information describing the workarea recovery site. If you need help to complete this template, please consult with your PC Support Team.It must contain the following information as a minimum:

Name of recovery vendor/premises	
Recovery Site Address	
Recovery site locality information and map	
Any other relevant information	

Appendices

This section can contain any relevant information. If you need help to complete this template, please consult with your PC Support Team. A few suggestions may be:

Printed copy of NDS	
Prints of start-up/autoexec files	
Total contents list of offsite vital records store	
Details of acceptance tests to be run once recovery is complete	

When complete, this form should be discussed with IT Services.

Midrange DR Components Specification Templates

The System

This section should contain information to generally describe the Midrange system. It must contain the following information:

Midrange system name: e.g.	
Where is it physically located?	
Location address:	
Contact names/Telephone numbers: ⇒ Administrator ⇒ Secondary Contact ⇒ Business Contact	
Owning Operating Company	

Equipment Schedule

This section should contain information to describe the Midrange system. It must contain the following information:

System make	
Model	
Relative performance	
Memory	
Disk capacity	
Number of CD-ROM	
Tape (1)	
Tape (2)	
Printer model	
Communications (1)	
Communications (2)	
LAN connected ?	
Modem	

Software requirements

This section should contain information describing what applications and software are required to be recovered on your system, including the operating system.

Software or application	**Version Number**	**Release Number**	**Comments**

Printer & Other Information

This section should contain information describing your printer requirements and any other hardware information (not already covered in 4.1).

Printer specification e.g. make/model e.g. HP laserjet 4	
Any other non-standard features, additional memory, etc.	

Invocation Procedures

The invocation procedure is usually detailed and provided by the third-party supplier but co-ordinated through IT Services.

Invocation procedure: Telephone call to: Information required to be supplied e.g. LAN name, location, etc: Authorised Business Personnel who can request invocation service:	
Non standard invocation procedures: - other technical supporting teams - other third party suppliers - recovery sites	

Vital Records & Backup Information

This section should contain information describing the your vital records store and backups taken of your system, applications and data files.

How do you take your backups ?	
What software is used (name/release/version) ?	
How can the passwords associated with the backups be obtained ?	
Where are the backup tapes kept ?	
Who or what procedure is used to take them to the offsite store ?	
What is the frequency of backup and does it depend on the day of the week, the week in the month and/or month in the year ?	
What other information is kept at the vital records store ? e.g. documentation, recovery procedures, timescales and priorities, business processes, etc. ?	
Detail information regarding the offsite store e.g. location address, passwords required, telephone numbers ?	
What is the retrieval procedure ?	
Who is authorised to retrieve the backups ?	
What other information do you have at the vital records store e.g. business processes documentation, recovery timetable, recovery procedures, etc.	

Recovery Site Information

This section should contain information describing the recovery site. It must contain the following information as a minimum:

Name of recovery vendor/premises	
Recovery Site Address	
Recovery site locality information and map	
Any other relevant information	

Appendices

This section can contain any relevant information. A few suggestions may be:

Total contents list of offsite vital records store	
Details of acceptance tests to be run once recovery is complete	

When complete, this form should be discussed with Information Technology Services.

BUSINESS CONTINUITY MANAGEMENT

The Companion Guide

SECTION FOUR:

GENERAL

Yellow Pages

Local Service Contacts

Glossary of Terms

Yellow Pages

Location Service Contacts

Service	Company	Contract Y or N ?	Contact	Telephone
Access Security				
Air-conditioning				
Building Maintenance				
Carpet Cleaning				
Catering				
Cleaners				
Cleaners - Window				
CCTV				
Computer Cleaning				
Duct Cleaning				
Engineering - Electrical				
Engineering - Maintenance				
Engineering - Mechanical				
Environmental				
Fire Detection/Alarm				
Gardener				
Generators				
Glazing				
Halon/Inergen Maintenance				
Heating				
Internal Plant Maintenance				
Laboratories				
Lift Maintenance				
Maintenance				
Oil				
PAT/Fixed or Hard wiring Services				
Photocopier/fax Maintenance				
Rubbish				
Safety Eye Maintenance				
Security - Guarding				
Skips				
Sprinkler Systems				
Telephone Switch Maintenance				
UPS				
Waste Disposal				
Waste Paper				
Water Detection Alarm				

Contacts

Service	Company	Contact	Telephone
Building Surveyor			
Fleet Management			
Furniture			
Human Resources			
Facilities Management			
Insurance			
Legal			
Loss Adjuster			
Salvage			

Local Services

Service	Company	Contact	Telephone
Airport			
Ambulance			
Bank			
Builders			
Builders Supplies			
Building			
Car Hire			
Carpentry			
Chemist			
Church			
Coach Hire			
Councillor			
County Council			
Courier Services			
Decorators			
DIY			
Doctors			
Electricity Board			
Emergency Signs			
Estate Agents Commercial			
Fire Service			
Gas Board			
Glazing			
Hospital			
Hotel			
Local Authority			
Locksmith			
Member of Parliament			
Newspaper			
Plant Hire			
Plumber			
Police			
Public House			
Pump Hire			
Radio			
Red Cross			
Removals			

Local Services (Continued)

Service	Company	Contact	Telephone
Royal Mail			
School			
Sports Centre			
Supermarket			
Taxi			
Telephones			
Television			
Train			
Water Company			
WRVS			

Glossary of Terms

contingency *n., pl.* **–cies. 1. a.** a possible but not very likely future event or condition; eventuality. **b.** *(as modifier): a contingency plan.* **2**. Something dependent upon a possible future event. **3.** A fact, event, etc., incidental to or dependent on something else.

The following terms are used throughout this Companion Guide. They are a mix of generally accepted terms and those that are specific to some businesses.

Alert	A situation in which Security have been informed of an incident and are considering the situation.
Alternate Site	A site held in readiness for use at Time of Disaster by an optimum number of staff in order to keep critical business processes going. The term applies equally to office or technology.
Assembly Area	The area at which staff congregate if evacuated. These locations are pre-agreed between Security and the Emergency Services.
Audit	The process by which procedures and/or documentation is measured against pre-agreed standards (1) The department within the business – which seeks to monitor and apply these standards (2)
Backup	A process by which data – electronic or paper based – is copied in some form so as to be available and used if the original data from which it originates is lost or destroyed.
Battle Box	A facility – often literally a box or filing cabinet – in which data and information is stored so as to be immediately available to the first response teams at Time of Disaster.
BCC	See Business Continuity Co-ordinator.
BIA	See Business Impact Analysis.
BRA	See Business Recovery Administrator.
Buddy	A scheme at Time of Disaster whereby individuals are paired for reasons of ensuring mutual safety and reporting to Emergency Marshals.
Business Continuity Management	The process by which an organisation prepares itself to be in a position to continue key business activities in the event of a disaster. This is the collective term used to combine Contingency Planning, Business Recovery Planning, Workarea Recovery Planning and Technology Recovery Planning.
Business Continuity Co-ordinator	The person who is responsible for ensuring that disaster recovery plans are built and implemented for a particular business area or Operating Company
Business Function	An entity, sometimes split across geographic boundaries, that has a distinct organisational function and a clear reporting line.
Business Impact Analysis	The process by which a business assesses the quantitative (financial) and qualitative (reputational) loss that might accrue if the business were to suffer a major disaster. The findings from a BIA are inevitably used to justify a Business Continuity Planning strategy and solution.
Business Interruption	The inability of a business to function for a period of time which typically threatens the well being of their business. The period will vary from business to business (1) ~ Planning: Synonymous with Business Recovery Planning (2)
Business Recovery	The process by which an organisation plans to recover from a business interruption or major disaster.
Business Resumption	Synonymous with Business Recovery
Campus	A set of buildings which are geographically grouped together. These buildings are either inter-dependent (i.e. if one fails they all fail) or are so close that a disaster at one would almost certainly impact at least one of the others. Typically these buildings would be within the same perimeter boundary. Explosive effects indicate that buildings must be at least 400 yards apart not to be guaranteed to be impacted at the same time.

Capital Investment	In a Business Continuity Planning sense this is the investment an organisation must spend in advance of a disaster to prepare for an incident.
Chief Emergency Marshal	Responsible for all the Emergency Marshals, the Chief Emergency Marshal is responsible for the evacuation procedure and reports any out-of-line situation or information received during evacuation to the Emergency Co-ordinator.
CIP	See Continuous Improvement Programme.
Cold Standby	A low-cost service operated by a third-party provider that provides space but no technology at time-of-disaster. Often mobile and delivered to the site of your choice they then need to be equipped with furniture and technology.
Command Centre	The place from which the recovery is managed and controlled by the CMT. It must be far enough away from the damaged site not to have been impacted by the event. May be one of a series to be selected at Time of Disaster depending upon the event.
Companion Guide	This manual. Provides a guide to Business Continuity Management.
Computer Centre	Any room which is equipped to house specialised technology. Often requires specialised environmental controlled atmosphere.
Contingency	Synonymous with first phase Crisis management procedures. The escalation, evacuation of staff.
Continuous Improvement Programme	CIP. The process of continually re-assessing BC strategies and solutions to ensure that we are getting best value from our Business Continuity Management approach and that plans are current and appropriate.
Control Group	This is the name that the CMT adopts on Day 2 of a disaster to impress on staff and our customers that we are in control of the incident.
Co-opted	Space occupied by staff that can be utilised by more essential staff from other business functions if those functions have suffered a disaster.
Corporate Affairs	Otherwise known as Public Relations. The art of ensuring that the staff, public, our clients and suppliers are kept informed of our progress at Time of Disaster with the minimum of fuss.
Cost Benefit	A study – part of the Risk Assessment process – where a case is made for Business Continuity Management solutions based upon the findings of the BIA.
Counselling	The process of helping those involved at times of crisis to manage their responses. Often most necessary several days after a disaster.
CPT	Contingency Planning Team. Exists to pre-plan and manage the Contingency Plan. At the time of an incident the chair will take central responsibility for co-ordination and will probably go on to chair the CMT.
Crisis Management	See Contingency. The process of managing non typical operational situations that threaten our staff and/or the business.
Critical	Usually applied to a resource or process that must be kept going (asap) at Time of Disaster.
Critical Business Activity	See above.
Criticality Analysis	The process of assessing which services and facilities are important to the continued well-being of the business.
Damage Assessment	A review of the impacted area of the business, both physical and economic, to assess what effect the incident has had on the business.
Data Centre	See Computer Centre.
Data Protection	Statutory requirements to manage personnel data in an open and appropriate manner that does not threaten or disadvantage its ‘owner’.
Denial of Access	The inability of a business to occupy its normal working environment. Usually imposed and controlled by the Emergency Services.
Desktop Services	Generally used to refer to PCs and services which reside in the user area.
Disaster	Any event which disrupts the business for a period exceeding the time that the business has stated that it can cope with an interruption.
Disaster Recovery	Synonymous with Business Continuity. Often applied specifically to IT recovery.
Distributed Systems	Those computer systems which are not located within a managed Computer Centre environment.
Emergency Control Centre	The Command Centre as used by the Contingency Planning Team during the first phase of an incident/disaster.
Emergency Co-ordinator	The person assigned the role of co-ordinating the activities of the Contingency Team with the business and Emergency Services.
Emergency Marshal	Operating under the direction of the Chief Emergency Marshal, the Emergency Marshals ensure that all staff, visitors and contractors evacuate the premises and reports to the Chief Emergency Marshal when their designated floor area is clear.

	Emergency Marshals should on completion of an evacuation report to the Chief Emergency Marshal the status of their area so that any unchecked areas of the building can be reported to the Emergency Co-ordinator who in turn will advise the Emergency Services when they arrive on site.
Emergency Response Procedures	The procedures used in the first phase response at Time of Disaster by the Contingency Team
Escalation	The process by which an incident is communicated upwards through the incident reporting chain of an organisation.
Evacuation	The movement of staff outside of the building to a safe place in a controlled and monitored manner at Time of Disaster.
Exercise	A way of testing part of a Business Continuity Plan. An exercise may involve invoking Business Continuity procedures but is more likely to involve the simulation of an event in which participants rôle-play in order to assess what the issues are, prior to a real invocation.
Expense Control	It is essential that ALL expenditures are carefully logged at time-of-disaster in a separate and distinct manner from the 'normal' procedure. The loss assessment and adjustment process will require this information to be readily available, once the recovery process is complete.
Facilities Management	The function which manages all aspects of the Company's infrastructure who play a pivotal role at Time of Disaster. This function is instrumental in assisting the damage assessment process at Time of Disaster and aiding the company to occupy either a new or a restored building post-disaster.
Fallback	Another term for alternative. The arrangements by which technology or facilities are made contingent. Another way of processing business. For example, a fallback computer system is another system that can be used when the original system is unusable or unavailable.
Facilities Management	Facilities Management
Gap Analysis	A survey which attempts to show the difference between **requirements** (what the business says it needs at Time of Disaster) and **availability (what would be available at Time of Disaster)**. Typically an analysis of workarea spaces, desktop equipment and centralised data Processing facilities. May vary between being a technical survey or simply a headcount survey. Used periodically to ensure that a Business Continuity solution keeps pace with organisational growth.
Green Tabard	Most buildings run on the principle of a Duty First Aider who will at the time of an evacuation take their first aid bag/box with them or collect one of the building first aid boxes and go to the Assembly Area or scene of incident, as appropriate. They should have a green tabard to wear in an evacuation so they can easily be identified. See Red Tabard.
Health & Safety	The process by which the well being of all staff and the public is safeguarded. All Business Continuity Plans and Planning must always be cognisant of H&S statutory & regulatory requirements. Business Continuity Planners must liaise with their local H&S officer.
Home Site	The primary site occupied by a business function. cf. Alternate or Secondary site.
Hot Standby	A term that can be applied to Business Continuity but is normally reserved for Technology Recovery. An alternate means of processing that minimises downtime so that no loss of processing time occurs. Usually involves the use of a standby system that is permanently connected to business users and is often used to record transactions in tandem with the primary system.
Housekeeping	The process of maintaining things in a repaired state. Applies to Systems as well as Business Continuity Plans.
HR	Human Resources (Personnel Department)
Incident Management	The process by which an organisation responds to and controls an incident. The result of a local event which threatens the well being of the business escalating into an event which requires the intervention of a management team. Synonymous with Crisis Management.
Infrastructure	A building and all of its supporting services including technology services. May be used within a technology context to mean those elements of the Data Processing environment that are fundamental to ther business's ability to continue to deliver Systems to the business community. Includes: the network (wide area and local area) as well as the computer configurations themselves.
Interim	If the Business Continuity strategy makes use of a commercial workarea &/or technical service provider, then such solutions are only available for a fixed period typically 8-12 weeks. The time between this initial occupation period and before returning to a new or refurbished home site, often requires an interim solution.
Invacuation	If the business is threatened by a potential bomb, Emergency Services may recommend moving staff to safer areas within the building rather than automatically evacuating staff. Unless specially built as such it should be assumed that there is no such thing as a 'safe'

	area. However, it is advisable to move staff away from obvious dangers such as windows etc. All Business Continuity Planners should be guided at all times by the Emergency Services and Security.
Invocation	The act by which a Business Continuity Plan is formally started. The term is often used to refer to the formal act of using a service such as Workarea recovery as offered by a commercial provider. All such acts should be formally notified by senior management often in the form of a Crisis Management Team.
Information Technology Recovery Planning	Procedures designed specifically to aid the recovery of Systems following an outage which impacts the ability of the business community to continue working. Often referred to as "Disaster Recovery Planning". IT or DR planning should always be seen as an integral part of Business Continuity Planning.
Key Task	Identified within a Business Continuity Plan as a priority action typically to be carried out within the first few hours of invocation.
LAN	Local Area Network. The cabling part of the infrastructure that provides the connectivity between desktop PCs and the computer providing the service ('Server').
Lead Time	The time it takes for a supplier – either of equipment or a service – to make that equipment or service available. Business Continuity Plans should try to minimise this by agreeing Service Levels with the supplier in advance of an incident rather than rely on the supplier's best efforts.
Legislative	Actions within a Business Continuity Plan that must be prioritised as a result of legal or statutory requirements.
Location	Used in the context of 'Primary' and 'Secondary' within Business Continuity Plans.
Loss Adjuster	Invaluable at Time of Disaster to assist the CMT in managing the financial implications of an incident. Try to involve the Loss Adjuster as part of the CMT. Loss Adjusters often have useful contacts within the local community that can ease the burden at Time of Disaster. Involving the Loss Adjuster with the CMT will improve the speed and effectiveness of any ensuing insurance claim.
Mainframe	A large centralised computer – housed in a Data Centre – that provides a System service to the business community. Unless fully resilient, requires an IT Recovery Plan in case of a major outage.
Manual Procedures	An alternative method of working following a loss of computer systems service. As working practices rely more and more on computerised activities the ability of an organisation to fall back to manual alternatives lessens. However, temporary measures and methods of working can help mitigate the impact of a disaster and give staff a feeling of doing something.
Marshal	Generally refers to an Emergency Marshal – typically at least one per business area-responsible for ensuring the smooth evacuation of staff and confirming that all staff are accounted for.
Media	News facilities including TV, Radio and newspapers. All media activity should be handled by Corporate Communications. Staff should be actively discouraged from talking to the media at Time of Disaster.
Mustering Point	A marked point to which all staff report to, following evacuation.
Needs Analysis	An assessment of business requirements – Desks, Telephones, PCs etc – that are needed by the business at Time of Disaster and at certain periods beyond. Sometimes considered to be part of a BIA. Is an integral part of any subsequent Gap Analysis.
Off-shore	Used in a Business Continuity Management context to refer to overseas business units, or a site external to a campus site.
Offsite	Mostly used to refer to a site where critical or important data (computerised or paper) is stored from where it can be recovered and used at Time of Disaster if original data and material is 'lost'.
Operating Company	Convenient term to refer to different parts of a business at a level higher than business function. Sometimes synonymous with Division.
Outage	Period of time that a system, service, process or business function is expected to be unusable or inaccessible.
PBX/PABX	Private (Automatic) Branch Exchange. Shorthand for the 'switchboard'. Requires a specific Business Continuity Planning solution as telephony is one of the first technical requirements of the business. Call Centres use the term Automatic Call Distribution (ACD) systems which require specialist recovery strategies.
PC Support Team	A team of PC specialists who provide support and technical knowledge to Desktop users
Plan Currency	Business Continuity Plans must be maintained (housekeeping) to an adequate state. The item within Business Continuity Plans that most commonly is not well maintained is the telephone contact details Business Continuity Plans should be maintained at least half-yearly and preferably quarterly.
Plan Maintenance	See Housekeeping. The act of keeping Business Continuity Plans up to date – the responsibility of the BCC.
Policy	A statement – usually expressed in high level terms – that is a requirement of the company for all employees to adhere to. Business Continuity Planning policy is documented in

	section A3 of this guide.
Portakabin	A temporary building used to house staff and or equipment that is erected, usually on a green field site, following an incident. The building may be used as an Alternate site or an Interim site. Portakabin is a commercial name and service that the R&SA has an existing SLA contract in place.
Post Disaster	The period of time (usually immediately) following an incident.
PR	Public Relations. A direct responsibility of the Corporate Communications function within the CMT.
Press Briefings	Pre-prepared statements issued to the press at Time of Disaster. Managed by Corporate Communications, no other statement will be made without the authority of senior management.
Preventative	Measures put in place to lessen the likelihood of an incident. A general term taken to mean Fire & Alarm procedures but also refers to new building methods which seek to 'build-in' protection. In a computer room environment it includes specialised environmental measures designed to stop incidents before they escalate into business threatening ones.
Prioritisation	Often part of a BIA in which computer systems and business tasks are ordered so that key systems and business tasks are addressed first at Time of Disaster.
Procurement	The process, managed by Facilities Management, by which replacement equipment, fixtures and fittings are bought following an incident. Business Continuity Management requires a quickened procurement process as the situation often dictates that normal procurement procedures are considered to be too slow.
Project Management	Business Continuity Management is a project like any other project. It involves a programme of work; produces deliverables; within a designated timeframe. This should be managed in a disciplined manner.
Public Data Services	Services, such as Teletext and others, which can be utilised at Time of Disaster to manage communication of the incident.
Public Relations	See PR.
Reciprocal	An arrangement by which one organisation agrees to use each others resources in the event of an incident. In a public context, this approach to Business Continuity Management is somewhat out of favour but can often be a useful internal Business Continuity Management solution. An approach that may well suit Call Centres who could redirect incoming calls around the network.
Recovery Management	The process by which a business manages its recovery (short and long-term) from an incident. Has three key components: Business Recovery, Workarea recovery, and Technology Recovery
Recovery Planning Life Cycle	The start to finish process by which the need for Business Continuity Plans are evaluated, developed, implemented and tested. A clearly defined programme that requires Project Management discipline to be successful. Once Business Continuity Plans are in place, the RPLC gives way to a Continuous Improvement Programme (CIP).
Recovery Point Objective	The point in time to which work should be restored following an incident that interrupts the business. In a Systems context this will be a pre-agreed point, for example: if a computer system goes down data is often recovered to start-of-day. In this case 'start-of-day' is the RPO or Recovery Point Objective. Determining the RPO, whether for computer or documented data, is an essential element of the Business Continuity Planning programme, part of the BIA process.
Recovery Strategy	The strategy – in terms of how, where and when to recover business activities following an incident – that is formally agreed and documented by the business.
Recovery Time Objective	The speed in which business and/or Systems are recovered at Time of Disaster. Determining the RTO, whether for computer systems or business, is an essential element of the Business Continuity Planning programme, part of the BIA process. Sometimes referred to as "time taken to recover" (TTR).
Recovery Timeline	The critical path of actions and activities which determine the speed and effectiveness of the recovery process.
Red Tabard	Emergency Marshals should be provided and wear red tabards at the time of an evacuation or when undertaking an Emergency Marshal role.
Regulatory	See Legislative.
Resource Pool	At Time of Disaster business recovery is conducted by business recovery teams. Resource Pool is often used to refer to staff not required in the initial period, often sent home, who will form the next wave of support brought in once the recovery process is underway.
Risk	Any threat to the business.
Risk Assessment	A process, within Business Continuity Planning often synonymous with a BIA, in which risks are reviewed to determine the likely impacts on the business.
Risk Management	A programme which seeks to put in place measures to address or mitigate those threats identified by the Risk Assessment.

Roll Call	Managed by Emergency Marshals, the process of ensuring that all staff have been safely evacuated following an incident.
Salvage	Dependent upon the type and severity of the disaster, recovery of personal effect, documentation and equipment may be possible. Specialist companies are ofgten used. Designated teams and staff will only take part in this process under the direction of the CMT and Emergency Services.
Security	The function which manages Security on behalf of the Company. Likely to be a key member of the Contingency Planning Team.
Service Continuity Co-ordinator	A term sometimes used to describe a BCC for a technical area such as Technology, i.e. the co-ordinator responsible for ensuring that a 'service' to the user community is maintained.
Service Level Agreement	A formal agreement between a service provider (whether internal or external) and their client (whether internal or external) which dictates the effectiveness of a service and the response of the service provider if the service is disrupted.
Standards	Statement of requirements designed to establish a minimum quality level against which Business Continuity Plans can be measured.
Synchronisation	Used to refer to a point in time, post disaster, at which Systems and business activities will be aligned. Dependent upon the RPO and RTO, it is essential that everyone involved in the recovery 'open their doors for business' at the same logical point.
Tasklist	A pre-written form used at time-of-disaster to ensure that those involved in the recovery do not miss items that need to be considered/addressed. Best kept in the Battle Box, A1 size for use at Emergency Control Centre.
Technology Recovery Planning	Same as Information Technology Recovery Planning
Template	A pro-forma Business Continuity Plan that can be used by BCCs to build their own area's Business Continuity Plan.
Test Plan	A programme of work designed to plan for testing a Business Continuity Plan.
Testing	The process by which strategies, solutions and documented Business Continuity Plans are tried out to ensure their success at Time of Disaster.
Third-Party	An external provider of BC services and solutions.
Time Taken to Recover	See RTO.
Time-of-Disaster	Abbreviated TIME OF DISASTER. Used in the phrase at TIME OF DISASTER. Means the time of the incident and/or point of invocation.
Vital Records	Computerised or paper records which are considered to be essential to the continuation of the business following a disaster (more usually used to refer to paper-based records). Business Continuity Planning programmes should include a Vital Records Programme as a matter of course. Solutions to addressing risks to Vital Records are often costly and involve long lead times to success.
Walkthrough	A way of exercising a Business Continuity Plan. Involves key participants checking through a Business Continuity Plan in a workshop environment. Often seen as the first part of a Business Continuity Plan testing programme. Should be undertaken before more costly exercises and tests are undertaken.
WAN	Wide Area Network. The communication links between R&SA buildings and the outside world. WANs can be either public or private networks. The R&SA use a mixture of both.
War Cabinet	Colloquial term for the CMT.
Warm Standby	An alternative Workarea/Data Centre that is not immediately occupiable/usable at Time of Disaster. Less expensive than Hot Standby, it is the most common form of externally provided Business Continuity Planning solutions. Most of these services involve a delay of between 4 and 24 hours before a working solution is ready.
Workarea	A pre-designated space, pre-provided with Desks, telephones and PCs, ready for occupation by business recovery teams at short notice. May be either internally or externally provided. Different levels of Workarea exist in terms of how quickly (compare Portakabin, Warm & Hot Standby) and what level of technology are immediately available.
Workarea Recovery Planning	The Business Continuity Planning process preparing procedures for the use of Workarea facilities.