ACKNOWLEDGEMENTS

The development of the Business Continuity Planning Guide (BCPG) was facilitated by PACE Central Advice Unit under the direction of the interdepartmental Joint User Group.

The members of the sub-group formed to provide an oversight of the drafting were:

Mr G. Bampton  Department of the Environment, Transport and the Regions
Mr S. Dilcock  Employment Service
Ms P. Elson  Government Historic Buildings Advisory Unit, English Heritage
Mr D. Flack  Ministry of Agriculture, Fisheries and Food
Mr G. Hodgkins  Home Office
Mr A. Howarth  Crown Prosecution Service
Mr A. Keen  Natural History Museum
Mr J. King  The Court Service
Mrs S. King  BMI Health Services (incorporating OHSA Limited)
Mr R. Law  Government Historic Buildings Advisory Unit, English Heritage
Mr S. Mack  National Monuments Record
Mr T. O’Reilly  Ministry of Agriculture, Fisheries and Food
Mr A. Rumsey  National Monuments Record
Mr T. Smith  Ministry of Agriculture, Fisheries and Food
Mr K. Wallace  Home Office
Mr S. Ramsden  PACE Central Advice Unit (Chairman)
Mr J. Ioannou  PACE Central Advice Unit
Mr T. Ross  PACE Central Advice Unit (Secretary)

The substantive drafting of the Guide was undertaken by Imbach RAG Ltd, Consultants, Challenge House, 616 Mitcham Road, Croydon, Surrey CR0 3AA.
Telephone: 0181 665 1459 Facsimile: 0181 665 1583

© Crown Copyright 1998
<table>
<thead>
<tr>
<th><strong>GLOSSARY</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Asset</strong></td>
</tr>
<tr>
<td><strong>Business Continuity (BC)</strong></td>
</tr>
<tr>
<td><strong>Business Continuity Plan</strong></td>
</tr>
<tr>
<td><strong>Business Continuity Team (BCT)</strong></td>
</tr>
<tr>
<td><strong>Business Unit</strong></td>
</tr>
<tr>
<td><strong>Contingency</strong></td>
</tr>
<tr>
<td><strong>Countermeasure</strong></td>
</tr>
<tr>
<td><strong>Damage</strong></td>
</tr>
<tr>
<td><strong>Damage Assessment</strong></td>
</tr>
<tr>
<td><strong>Disaster</strong></td>
</tr>
<tr>
<td>Term</td>
</tr>
<tr>
<td>--------------------------</td>
</tr>
<tr>
<td>Essential Operations</td>
</tr>
<tr>
<td>Incident</td>
</tr>
<tr>
<td>Incident Control</td>
</tr>
<tr>
<td>Incident Control Room</td>
</tr>
<tr>
<td>Incident Control Team</td>
</tr>
<tr>
<td>Invoke</td>
</tr>
<tr>
<td>Likelihood</td>
</tr>
<tr>
<td>Maximum Acceptable</td>
</tr>
<tr>
<td>Outage Time</td>
</tr>
<tr>
<td>Operation</td>
</tr>
<tr>
<td>Recovery Centre</td>
</tr>
<tr>
<td>Recovery Planning</td>
</tr>
<tr>
<td>Recovery Strategy</td>
</tr>
</tbody>
</table>
Recovery Team  a pre-selected group to carry out the recovery actions necessary to resume business operations. Typically there would be one Recovery Team for each business unit at a premises, recovering the major operation or operations of that area, and usually composed of senior staff from that business unit.

Risk  the exposure to unwanted loss. It is the measure of the likelihood and the consequence if a particular threat is realised.

Risk Assessment  the process of identifying and analysing the risks faced by an organisation.

Risk Management  an ongoing method within an organisation for reviewing, reducing and controlling risks.

Strategy  see Recovery Strategy.

Task List  the list of actions for a Recovery Team to carry out in order to restart business. The Task List is the core of the Business Continuity Plan. Tasks are
- in logical order;
- what needs to be done, not how to do it.

Threat  anything with potential for adverse effect on an asset, for example fire, unauthorised access to premises.

Vulnerability  susceptibility of an asset to a threat, for example no sprinkler system to protect against fire.
# ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BCP</td>
<td>Business Continuity Plan</td>
</tr>
<tr>
<td>BCPG</td>
<td>Business Continuity Planning Guide</td>
</tr>
<tr>
<td>BCT</td>
<td>Business Continuity Team</td>
</tr>
<tr>
<td>BIR</td>
<td>Business Impact Review</td>
</tr>
<tr>
<td>CAU</td>
<td>Central Advice Unit (PACE)</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed Circuit Television</td>
</tr>
<tr>
<td>ESG</td>
<td>The Estates Services Guide</td>
</tr>
<tr>
<td>GACC</td>
<td>Guide To The Appointment Of Consultants And Contractors</td>
</tr>
<tr>
<td>GTN</td>
<td>Government Telephone Network</td>
</tr>
<tr>
<td>IC</td>
<td>Incident Control</td>
</tr>
<tr>
<td>ICT</td>
<td>Incident Control Team</td>
</tr>
<tr>
<td>JUG</td>
<td>Joint User Group</td>
</tr>
<tr>
<td>MAOT</td>
<td>Maximum Acceptable Outage Time</td>
</tr>
<tr>
<td>PACE</td>
<td>Property Advisers to the Civil Estate</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PMG</td>
<td>The Premises Management Guide</td>
</tr>
</tbody>
</table>
**SECTION ACRONYMS**

The following acronyms are used in cross references to other parts of the Guide:

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABOUT</td>
<td>About this Guide</td>
</tr>
<tr>
<td>BIR</td>
<td>Business Impact Reviews</td>
</tr>
<tr>
<td>CONT</td>
<td>Contingency Considerations</td>
</tr>
<tr>
<td>IC</td>
<td>Incident Control</td>
</tr>
<tr>
<td>INT</td>
<td>Interim Business Continuity Plans</td>
</tr>
<tr>
<td>INTRO</td>
<td>Introduction</td>
</tr>
<tr>
<td>OVER</td>
<td>Overview of Plan Development and Strategy Considerations</td>
</tr>
<tr>
<td>PLAN</td>
<td>Plan Development and Implementation</td>
</tr>
<tr>
<td>REC</td>
<td>Recovery Strategy</td>
</tr>
<tr>
<td>RISK</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>TEST</td>
<td>BCP Awareness, Testing, Training and Maintenance</td>
</tr>
</tbody>
</table>
CONTENTS

ABOUT THIS GUIDE

BACKGROUND TO THE GUIDE
PURPOSE OF THE GUIDE
STRUCTURE OF THE GUIDE

INTRODUCTION (INTRO)  1.0

ABOUT THIS SECTION  1.1
WHAT IS A DISASTER?  1.2
WHAT IS BUSINESS CONTINUITY PLANNING?  1.3
FEATURES OF BUSINESS CONTINUITY PLANNING  1.4
WHAT IS INCIDENT CONTROL?  1.5

OVERVIEW OF PLAN DEVELOPMENT AND STRATEGY CONSIDERATIONS (OVER)  2.0

ABOUT THIS SECTION  2.1
CONSIDERING THE IMPACT OF A DISASTER  2.2
PHASES OF A DISASTER  2.3
POSSIBLE COMBINATIONS OF PHASES OF A DISASTER  2.4
DEVELOPMENT PROCESS OF BUSINESS CONTINUITY PLANNING  2.5
TYPES OF BUSINESS CONTINUITY PLANS  2.6
STRATEGY CONSIDERATIONS  2.7
INITIAL PREPARATIONS  2.8
ROLES AND RESPONSIBILITIES  2.9
WHAT SHOULD YOU DO?  2.10
RISK ASSESSMENT (RISK) 3.0

ABOUT THIS SECTION 3.1
WHAT IS RISK ASSESSMENT? 3.2
WHAT IS AN ASSET? 3.3
WHAT IS A THREAT? 3.4
RISK ASSESSMENT METHODS 3.5
CONDUCTING A RISK ASSESSMENT 3.6
RISK MANAGEMENT 3.7
CHOOSING COST-EFFECTIVE COUNTERMEASURES 3.8
LEARNING FROM EXPERIENCE 3.9
WHAT SHOULD YOU DO? 3.10
RISK ASSESSMENT WORKSHEET ANNEX 3/1

BUSINESS IMPACT REVIEWS (BIR) 4.0

ABOUT THIS SECTION 4.1
BUSINESS IMPACT REVIEW INTERVIEWS 4.2
COMPARING THE IMPACT OF OPERATION STOPPAGES 4.3
ASSESSING THE IMPACT OF OPERATION STOPPAGES 4.4
IDENTIFYING ESSENTIAL OPERATIONS 4.5
BUSINESS IMPACT REVIEW REPORT 4.6
WHAT SHOULD YOU DO? 4.7
BUSINESS IMPACT REVIEW - INTERVIEW WORKSHEET ANNEX 4/1
BUSINESS IMPACT REVIEW - IMPACT WORKSHEET ANNEX 4/2
BUSINESS IMPACT REVIEW - OPERATION SUMMARY WORKSHEET ANNEX 4/3

CONTINGENCY CONSIDERATIONS (CONT) 5.0

ABOUT THIS SECTION 5.1
USE OF CONTINGENCIES 5.2
TYPES OF CONTINGENCIES 5.3
IDENTIFYING MINIMUM REQUIREMENTS 5.4
CONSIDERING SUITABLE CONTINGENCIES 5.5
EVALUATING AND CHOOSING SUITABLE CONTINGENCIES 5.6
WHAT SHOULD YOU DO? 5.7
RECOVERY STRATEGY (REC) 6.0

About This Section 6.1
Main Sources of Information 6.2
Identifying Alternative Strategies 6.3
Compiling a Cost-Effective Recovery Strategy 6.4
The People Factor 6.5
Recovery Strategy Report and Management Decision 6.6
Implementing the Strategy 6.7
What Should You Do? 6.8

PLAN DEVELOPMENT AND IMPLEMENTATION (PLAN) 7.0

About This Section 7.1
Structure and Content of the BCP Document 7.2
Writing the BCP 7.3
Recovery Team Composition 7.4
Recovery Team Tasks 7.5
Review of First Draft 7.6
Implementation and Testing 7.7
Distribution 7.8
Version Control 7.9
What Should You Do? 7.10
Specimen Plans ANNEX 7/1

BCP AWARENESS, TESTING, TRAINING AND MAINTENANCE (TEST) 8.0

About This Section 8.1
Creating Awareness 8.2
Testing 8.3
Training the Recovery Teams 8.4
Exercise Methods 8.5
BCP Maintenance 8.6
What Should You Do? 8.7
Sample Scenario ANNEX 8/1
INTERIM BUSINESS CONTINUITY PLANS (INT) 9.0

About this Section 9.1
Purpose of an Interim Business Continuity Plan 9.2
Developing an Interim Business Continuity Plan 9.3
What Should You Do? 9.4
Example of an Interim Business Continuity Plan Annex 9/1

INCIDENT CONTROL (IC) 10.0

About this Section 10.1
Purpose of Incident Control 10.2
Incident Control Team 10.3
Incident Control Team Action 10.4
Emergency Procedures 10.5
Additional Considerations 10.6
Incident Control Manual 10.7
Incident Control Room 10.8
Damage Assessment and Salvage 10.9
What Should You Do? 10.10
Sample Incident Control Procedures Annex 10/1
ABOUT THIS GUIDE

INTRODUCTION
BACKGROUND
BUSINESS CONTINUITY PLANNING GUIDE
PURPOSE OF THE GUIDE
STRUCTURE OF THE GUIDE
ABOUT THIS GUIDE

INTRODUCTION

Property Advisers to the Civil Estate (PACE) is an executive agency of the Cabinet Office (Office of Public Service). Its main aim is to enable Departments to achieve best overall value for money in the management of their property assets by providing a range of co-ordination and advisory services. PACE also has a key role in facilitating co-operation between Departments on their property decisions in order to optimise Exchequer savings.

PACE’s advisory services are designed to support Departmental Premises Managers by providing a full range of property-related advice through the issue of Guides, Bulletins, Information Notes and Health and Safety Alert Notices. PACE’s advice encompasses the areas of estate and property management and the related areas of procurement, forms of contract and procedures on property and works issues for those clients who do not have the necessary expertise to carry out the “intelligent client” role in-house. PACE can provide these services on a repayment basis. The service can range from dealing with a single project, perhaps on a project sponsorship basis, through support in commissioning managing agents, advice on property-related PFI proposals, to a full service dealing with all property management issues.

BACKGROUND

Development of the Business Continuity Planning Guide (BCPG) was facilitated by PACE Central Advice Unit under the direction of the Joint User Group comprising representatives from a range of property-owning Departments, with the substantive drafting being undertaken by consultants specially commissioned for the project.
BUSINESS CONTINUITY PLANNING GUIDE

The BCPG was produced in response to requests from Departments for guidance in preparing Business Continuity Plans for premises for which they have a management responsibility. It encourages them to plan against, and recover from, the effects of an incident at a property on their estate in a cost-effective manner and offers advice in carrying out Risk Assessments and also in producing interim Business Continuity Plans for premises which are considered to be particularly at risk pending the production of full Plans.

It is one in a series of Guides being developed by PACE’s Central Advice Unit as a family of guidance documents. These include the Premises Management Guide, the Estates Services Guide, the Guide to the Appointment of Consultants and Contractors and the Fire Safety Guide. Substantial cross referencing exists between the Guides.

PURPOSE OF THE GUIDE

The BCPG is intended to assist Departments in preparing Business Continuity Plans for their premises and can be used to form the basis of a structured approach to undertaking this exercise by offering comprehensive, practical guidance in producing these Plans.

The BCPG will be updated from time to time, when necessary and CAU will publish relevant details of any important changes.

Following requests from Departments for assistance in preparing Business Continuity Plans the Central Advice Unit (CAU) Advisory Panel asked PACE to produce a framework guide which Departments can adapt for their own purposes. The preparation of the Guide has been overseen by the Joint User Group (JUG) consisting of representatives of the main property owning Departments. The Guide was commissioned by the CAU from Imbach RAG Ltd and much valuable assistance with its detailed drafting was provided by the Guide sub-group of the JUG.
Business Continuity planning involves everyone and everything in a property: although Premises Managers often act as facilitators for BCP projects, they are not intended to have sole responsibility for the planning of Business Continuity.

This Guide is intended to assist all managers involved in the preparation of BCPs by explaining the concepts and reasons for Business Continuity Planning, Risk Assessment and Management and Incident Control, by demonstrating how:

- risk reduction techniques will reduce the likelihood of a risk becoming a reality;
- Incident Control will help to lessen the effects of a disastrous incident; and
- a BCP will direct the restarting of operations.

The BCPG is intended for the lay reader with no prior knowledge of the subject. It will enable:

- a comprehensive Recovery Planning exercise to be carried out which, by addressing all the relevant topics, will result in the drawing up of plans for the continuity of essential operations throughout a disaster;
- a basic Interim Plan to be put in place quickly in advance of the full BCP if there is a high and immediate risk to the premises or operations.

In its advisory role PACE is the owner of this Guide, which is available from PACE on request. The use of this guide is not mandatory but optional.
STRUCTURE OF THE GUIDE

This Guide is divided into 11 sections:

- **About this Guide**, which gives an explanation of the Guide's purposes;
- **Section 1 - Introduction** which gives an introduction to Business Continuity Planning and Incident Control;
- **Section 2 - Overview of the Development Cycle**, which gives the basic concepts and pre-requisites for developing recovery planning;
- **Section 3 - Risk Assessment and Management**, which explains how Risk Assessment and Management can reduce the threat of a risk becoming a disaster;
- **Section 4 - Business Impact Review**, which explains how to plan and conduct a Business Impact Review;
- **Sections 5 to 8** deal with successive stages of the development process for the BCP;
- **Section 9 - Interim Plan**, which contains an example of an Interim Plan which can be brought into immediate temporary use if Departments feel that particular premises are particularly vulnerable to a disaster;
- **Section 10 - Incident Control**, which explains how to set up procedures to deal with a physical crisis at the premises.

Each section starts with **About this Section**, which contains:

- an explanation of the section subject matter; and
- key points which are explained more fully in the text of the section.

Each section ends with:

- a list of actions headed **What Should You Do?**; and
- any annexes appropriate to the section, for example specimen worksheets, Plans, etc.
The top of each page has an index card icon showing the current section and sub-section. At the bottom of the page is the:

- issue number and date of issue of the Guide; and
- section acronym and page number.

The right hand margin may contain, as appropriate, icons relating to the adjoining text:

- the warning triangle indicates where particular care needs to be taken to ensure that the relevant action is being taken;
- this icon indicates cross references to other related sections of the Guide. The reference in the icon is the section and section number. Alternatively, the icon may refer to another PACE CAU guide;
- the open book icon indicates where a reference to other documents or further reading is made.
1.0 INTRODUCTION

1.1 About this Section

1.2 What is a Disaster?

1.3 What is Business Continuity Planning?

1.4 Features of Business Continuity Planning

1.5 What is Incident Control?
1.0 INTRODUCTION

1.1 ABOUT THIS SECTION

This section includes:

• an explanation of what is meant by 'disaster';

• a summary of the three complementary features involved in Business Continuity Planning for recovery from a disaster:
  - prevention;
  - Emergency Plan;
  - Business Continuity Plan (BCP); and

• an explanation of Business Continuity Planning and Incident Control.
1.2 WHAT IS A DISASTER?

For the purpose of this Guide, a disaster is an incident or event which:

- threatens personnel, buildings or the organisational structure of an organisation; and
- requires special measures to be taken to restore things back to normal.

There are many possible causes of a disaster or disruptive event which occurs or threatens to occur to the premises, and the extent of their impact will vary from incident to incident. The most likely causes a Department will be faced with are:

- fire;
- flood;
- storm;
- bomb threat;
- bomb damage;
- vandalism, for example broken glass making the entrance unsafe to use;
- heating or air conditioning failure which could lead to staff walkout;
- power failure;
- inclement weather;
- loss of essential services, such as power, telephones or lifts; or
- asbestos discovery in older premises.
1.3 WHAT IS BUSINESS CONTINUITY PLANNING?

Business Continuity Planning, that is, planning for recovery from a disaster, aims to:

• manage the risks which could result in disastrous events and thus minimise the likelihood of a disaster occurring;

• reduce the time taken to recover when an incident occurs; and

• minimise the risks involved in the recovery process by making the critical decisions in advance in stress-free conditions.

Critical decisions made during the stress of a crisis have a high risk of being wrong, ineffective, and costly.

Although the likelihood of a disaster occurring at a specific property is low, it could, and does, happen at any time. The problem facing Departments is what to do when their premises are left unusable for an unacceptable length of time. The intention will be to restart essential operations with a minimum of delay within an acceptable length of time, probably with a reduced capacity in temporary premises.

Departments, and their Premises Managers in particular, need to know what is expected from them during and immediately after a disaster; before full restoration of existing facilities. Business units need to determine their minimum requirements and agree the recovery Plan before Departments can make their own Plans to support the recovery.
1.4 FEATURES OF BUSINESS CONTINUITY PLANNING

Business Continuity Planning has three complementary features:

1. **Risk reduction** - the management of risks to prevent a disaster. This is done by identifying and assessing the risks faced by a Department at their premises which could result in a disaster;

2. **Emergency Plan** - crisis management of the incident when it occurs (Incident Control) to prevent it from developing into a disaster, and to lessen its impact. The priority is to evacuate staff and others when this is necessary, but essential or valuable information and objects can often be rescued without risk to personal safety;

3. **Business Continuity Plan** - a Plan for the fast, efficient resumption of essential business operations by directing the recovery actions of specified recovery teams. The three elements to consider are the continuity of:
   - **office services** - premises, furniture, stationery etc;
   - **information technology** - communications and computing services; and
   - **human and other resources** - ensuring that staff:
     - are aware of the alternative arrangements;
     - have the resources they need; and
     - are productively employed.

The key tasks in Business Continuity Planning are to:

- identify which operations and supporting activities need to be restarted after a disaster, the maximum acceptable time limits by which they must restart, and the resources needed to restart them;
- identify contingencies for the required resources;
- select a cost-effective strategy for restarting operations;
- develop the BCP to guide and direct the restart of operations;
- test the BCP, train staff in how to use it, and keep it up to date.
1.4.1 The Business Continuity Plan

If a BCP is to be correctly constructed and operate successfully, it must involve all levels of management, and must cover the:

- action to be taken following a disaster;
- staff responsible for specific tasks;
- essential operations and systems;
- actions required to restart operations;
- emergency data processing arrangements;
- off-site backup requirements;
- supplies requirements; and
- means of keeping staff and others informed of arrangements and developments.
1.5 WHAT IS INCIDENT CONTROL?

An Incident Control function is set up to provide an emergency response to a physical crisis at the premises which is causing, or threatening to cause, a disaster, for example a fire or flood.

The most important objective of Incident Control is to ensure the preservation of life by:

- preventing injury;
- providing shelter; and
- evacuating the premises, if necessary.

Other objectives of Incident Control are to:

- prevent the incident from escalating into a disastrous event;
- reduce and control the effects of the incident; and
- make sure salvage and repairs are started at the earliest opportunity.

Incident Control does not replace the Emergency Services. For example, if fire is threatened or has broken out, the Fire Service must be called and Incident Control must work with, or around, them as appropriate.

The presence of an Incident Control function will reduce the likelihood of the BCP being invoked.
2.0 OVERVIEW OF PLAN DEVELOPMENT AND STRATEGY CONSIDERATIONS

2.1 ABOUT THIS SECTION
2.2 CONSIDERING THE IMPACT OF A DISASTER
2.3 PHASES OF A DISASTER
2.4 POSSIBLE COMBINATIONS OF PHASES OF A DISASTER
2.5 DEVELOPMENT PROCESS OF BUSINESS CONTINUITY PLANNING
2.6 TYPES OF BUSINESS CONTINUITY PLANS
2.7 STRATEGY CONSIDERATIONS
2.8 INITIAL PREPARATIONS
2.9 ROLES AND RESPONSIBILITIES
2.10 WHAT SHOULD YOU DO?
2.0 OVERVIEW OF PLAN DEVELOPMENT AND STRATEGY CONSIDERATIONS

2.1 ABOUT THIS SECTION

This section gives:

- an explanation of how Business Continuity Planning is influenced by an understanding of the implications of a disaster. This includes:
  - the impact of a disaster; and
  - the phases a disaster may go through;
- an overview of how to develop a Business Continuity Plan (BCP);
- a summary of the stages involved in developing a BCP; and
- information about:
  - involvement of management;
  - types of BCP;
  - strategy considerations;
  - initial preparations for planning; and
  - roles and responsibilities.

2.1.1 Key Points

The key points to note for BCP development and strategy considerations are that:

- for Business Continuity purposes it is the damage and impact of the event which is important, not the cause;

- the physical damage to premises caused by a disaster will be addressed by the restoration process;

- all management at the premises must be involved in planning the BCP development project; and

- the first step in starting the BCP development project is to establish the Project Owner, the Business Continuity Officer, the Objectives and the Scope.
2.2 CONSIDERING THE IMPACT OF A DISASTER

When considering the impact of a disaster, it should be remembered that it:

• will never happen at a convenient time; and
• is always unpredictable. There is no way of knowing:
  - when it will happen;
  - what form it will take;
  - how much damage it will cause; or
  - how big the impact will be.

The impact of a disaster can vary. A disaster could involve:

• **total destruction** of the premises and its contents, for example as a result of a serious fire;

• **partial damage**, preventing use of the premises, for example through flooding; or

• **no actual physical damage** to the premises but restricted access for a limited period, such as enforced evacuation due to the discovery nearby of an unexploded World War Two bomb.

For Business Continuity purposes, it is not the cause of the event which matters but the damage and impact from it. The BCP is unlikely to be invoked if normal working can restart in the premises within a reasonable time, for example 48 hours.
2.3 PHASES OF A DISASTER

A typical disaster will consist of some or all of the following phases:

- Crisis Phase;
- Emergency Response Phase;
- Recovery Phase; and
- Restoration Phase.

2.3.1 Crisis Phase

The Crisis Phase is under the overall responsibility of the Incident Control Team (ICT). It:

- comprises the first few hours after a disruptive event starts or the threat of such an event is first identified; and
- is caused by, for example:
  - ongoing physical damage to premises which may be life threatening, such as a fire; or
  - restricted access to premises, such as a police cordon after a bomb incident or discovery of asbestos in the premises.

During the Crisis Phase:

- the Fire And Other Emergency Evacuation Procedures (including Bomb Threat and Valuable Object Removal Procedures) will apply; and
- the emergency services should be summoned as appropriate.
2.3.2 Emergency Response Phase

The Emergency Response Phase may last from a few minutes to a few hours after the disaster. It will start near the end of, or after, the Crisis Phase if there has been one, or when a potentially threatening situation is identified.

During the Emergency Response Phase the Business Continuity Team (BCT) will:

- assess the situation; and
- decide if and when to activate the BCP.

A Crisis Phase may not actually have occurred but a potentially threatening situation may have been identified which would warrant calling out the BCT to monitor events, for example a fire has broken out in the building next door which, if not brought under control quickly, may damage Departmental premises and will certainly require evacuation procedures to be invoked.

2.3.3 Recovery Phase

The Recovery Phase may last from a few days to several months after a disaster and ends when normal operations can restart in the affected premises or replacement premises, if appropriate.

During the Recovery Phase:

- essential operations will be restarted (this could be at temporary premises) by one or more Recovery Teams using the BCP; and
- the essential operations will continue in their recovery format until normal conditions are resumed.

2.3.4 Restoration Phase

This phase restores conditions to normal. It will start with a damage assessment, usually within a day or so of the disaster, and may identify any need for refurbishment or even replacement of the premises.

This phase will not occur if physical damage did not happen. When the cause for evacuation or stopping of operations has ended, normal working will be restarted. During the Restoration Phase any damage to the premises and facilities will be repaired.
POSSIBLE COMBINATIONS OF PHASES OF A DISASTER

Because each disaster is different:

- it is not possible to predict which phases a disaster will involve; and
- the response to an incident will vary according to the individual circumstances.

Some examples of disasters and the phases they may involve are:

- serious fire during working hours - all the phases in full;
- serious fire outside working hours - all the phases but no staff and public evacuation;
- very minor fire during working hours - Crisis Phase only, staff and public evacuation but perhaps no removal of valuable objects, Fire Service summoned to deal with the fire;
- gas main leak in street outside working hours, repaired after some hours - only Emergency Response Phase appropriate. The BCT monitors the event against the need to invoke the BCP, with the ICT on standby; and
- prolonged failure of heating system during winter – Emergency Response and Recovery Phases only.
DEVELOPMENT PROCESS OF BUSINESS CONTINUITY PLANNING

2.5

OVERVIEW OF PLAN DEVELOPMENT AND STRATEGY CONSIDERATIONS

2.5.1

Involvement of Management

The first stage in the development of planning for continuity is to allocate correctly the responsibility for delivery of the BCP project.

The managers of all the Department's operational units should be involved in the discussion of the planning because:

- a disaster could affect their activities to a lesser or greater degree, depending on the scale of the disaster; and
- co-ordination in planning is essential for successful recovery.

This involvement and commitment by all levels of management will be necessary for the successful conclusion of the planning activities.

Risk Assessment, Business Continuity Planning and Incident Control should be seen as a mission-critical senior management exercise.

Management at each property should:

- identify someone with the right skills, knowledge and ability for the task of Business Continuity Planning. They would usually be someone with the appropriate management position and experience; and
- consider carefully before delegating the responsibility down to a level below management, as the quality of the work and therefore of the finished BCP will reflect the skills and abilities of the person(s) carrying out the work.

It should be remembered that the annual costs and effort in respect of maintenance, testing and training in connection with Business Continuity will be much lower after the initial development of the BCP.
2.5.2 Development Phases

The recommended way to produce a BCP is to work through the successive development phases explained below and shown in the flowchart at OVER 2.5.3.

A written report should be:

• produced at the end of each phase;

• agreed by all management concerned before starting the next phase; and

• used as input for the next phase.

The development phases are:

1. Initial Preparation - involves all senior management in the:
   • development of the Business Continuity Planning project;
   • assignment of a Project Owner to take responsibility for it;
   • agreement of objectives and scope for the project; and
   • appointment of a Business Continuity Officer to organise and supervise the preparation work;

2. The Interim Plan - a stop-gap, emergency-only Plan for use during the preparation stage of a BCP if it is felt that premises are particularly vulnerable to a disaster during the time it will take to produce a properly developed BCP. The Interim Plan must never be retained as a substitute for a properly developed BCP;

3. Risk Assessment - this phase provides input to risk management by identifying and evaluating:
   • the risks to the premises and its operations; and
   • any cost-effective measures for prevention which can be put into place.

An effective Risk Assessment reduces the likelihood and impact of a disaster and the need to call out the Incident Control or the Business Continuity Teams;
4. **Business Impact Review** - identifies the essential operations and the impact and Maximum Acceptable Outage Time (MAOT) for each essential operation, for example, the possible effect on business units if the Reprographics room became unusable;

5. **Contingency Considerations** - identifies the various options for obtaining replacement or substitute resources to aid recovery from the loss of the original resources. Using the Reprographics example above, this could mean finding a print shop nearby which can do all the reprographics work;

6. **Recovery Strategy** - identifies and compares the various recovery options to establish which are the most efficient and cost-effective. It will recommend for management’s approval the strategy felt to best meet the requirements. Again using the example above, this could mean finding a cheaper reprographics service;

7. **Plan Development and Implementation** - produces the actual BCP and gets the key people involved;

8. **Awareness, Testing, Training and Maintenance** - awareness of the Business Continuity Planning project and its purpose should be promoted at every opportunity, as awareness at all staff levels contributes to successful recovery from a disaster:

   Testing the **BCP** and training staff to use it are necessary to ensure that recovery will happen as expected. Every training session helps to test the **BCP** and every test helps to train the participants.

   The **BCP** must be reviewed and maintained regularly if it is to remain effective and relevant.
2.5.3 Flowchart of BCP Development Process

1. Initial Preparations

3. Risk Assessment

4. Business Impact Review

5. Contingency Considerations

6. Recovery Strategy

7. BCP Development

8. Awareness, Testing, Training, Maintenance, Review

2. Interim Plan
2.6 TYPES OF BUSINESS CONTINUITY PLANS

The type of BCP needed will depend on the size and complexity of the premises and operations within it. For smaller, simpler premises a single BCP containing Task Lists for the BCT and the Recovery Team(s) may be sufficient.

However, for more complex situations a separate Plan for each business unit may be appropriate. These Plans should be consistent in style and work together to form a comprehensive recovery Plan for the whole premises.

For large complex premises a three level Plan may be appropriate:

1. **Top level - Premises Plan** for management and the BCT. This will invoke the second level of Plans, one for each of the major operational areas within the premises, for example, the Finance area;

2. **Second level - Area Plan** covers the management of the recovery of operations within that area and invokes the business unit level Plans for individual operations, for example Payroll operations within the Finance area; and

3. **Third level - Business Unit Plan** covers one or more of the individual operations, for example Payroll.

Each Plan at any level should have its own Recovery Team.

Any combination of the levels is possible, provided the resulting Plans cover all essential operations.
2.7 STRATEGY CONSIDERATIONS

Management responsible for business units need to:

- agree the level and urgency of recovery necessary for Business Continuity; and
- choose a strategy which will produce that recovery.

The Business Impact Review (BIR) will have identified the critical operations and their respective time limits for restarting. The Recovery Strategy will have established the minimum number of staff necessary for each operation to continue. Providing facilities for this minimum number will be more cost-effective for the business than trying to get all the staff back to work.

To be able to choose the best strategy there must be a balance between:

- cost;
- numbers of staff;
- time limits; and
- degree and certainty of recovery.

Generally, more comprehensive and well thought-out strategies produce faster and more dependable recovery, while simpler strategies take longer and may not guarantee success within time and cost.

If valuable objects or information are on the premises:

- incident prevention and the speed and type of response will have much higher priority than in a typical office environment; and
- procedures should exist to cover the prompt and safe removal of the objects. Crisis procedures for dealing with valuable objects should be independent from, but coordinated with, the BCP. This is because of the specific purpose of removing the valuable objects and the potential need for an urgent response.

Incident Control procedures should already be in place to cover incidents such as Bomb Threat or Emergency Evacuation. These procedures should also be independent of the BCP.
2.8 INITIAL PREPARATIONS

The following preparations for planning are highly recommended to ensure a good start to the process of producing a BCP.

2.8.1 Ownership

Ownership is the recommended means for ensuring that the development project and finished BCP receive all necessary support and awareness. Separate owners for the BCP development project (Project Owner) and the BCP itself (Business Continuity Officer) should be established at the appropriate level and agreed by management. With separate Project Owners and Business Continuity Officers, ownership can be set at an appropriately high level. In practice, however, Project Owners will oversee and delegate to the Business Continuity Officers.

2.8.2 Objectives and Scope

Every BCP development project should start with:

- an agreed statement of its objectives and scope;
- a completion date; and
- a list of the key people to be involved.

It could also include statements on roles and responsibilities, and on ownership. The Project Owner and/or the Business Continuity Officer would be responsible for the preparation of this document and for obtaining approval for it from all management concerned.

Each of the development phases described in section OVER 2.5.2 should be planned as a project in its own right.
Example of Objectives and Scope for a Business Continuity Plan Development Project

The following example can be used as the basis for drafting a document specific to the Department or business unit and property, but should not be used without alteration to suit particular premises, as circumstances will vary from Department to Department and from property to property.

### Objectives of the Development

1. To create BCPs which will enable the critical operations carried out by [name of Departmental operational area] at [name of premises] to be restarted after any disaster which has prevented them from continuing at their current location.

2. BCPs should be developed and drafted to a quality such that:
   a. the recovery of the services provided by [name of Departmental operational area] will be such that users of the services would otherwise be unaware of the disaster;
   b. recovery takes place as expected; and
   c. the recovery processes are efficient and cost-effective.

3. In preparation for developing the Plans, the following should be identified:
   a. critical operations which will need to be recovered;
   b. time limit within which each operation must be recovered; and
   c. minimum resources required by each operation to enable its recovery.

4. To make Plans to acquire, or enter into contracts to provide, the contingency resources needed to achieve recovery should the original resources become unavailable because of the disaster.
5. To conduct a review of the risks faced by [name of Departmental operational area] at [name of premises] with the objective of identifying and assessing them in order to:
   a. reduce them to an acceptable level meeting all legal requirements; and
   b. reduce the likelihood of a disaster happening at [name of premises] by managing the threats which cause the risks.

6. When the BCPs have been created, to:
   a. test them;
   b. train staff in their use of them; and
   c. regularly review and maintain them so that they remain efficient and cost-effective.

Scope of the Development

1. The entire premises at [name of premises] and the operations carried out there will be included in the development processes.

2. All of the management of [name of Departmental operational area] at [name of premises] will be involved in the development and the decisions relating to the development processes.

3. The completion date for having the Plans in place and tested is [dd/mm/yy].

Personnel Required for the Development

The personnel who will be involved in the development are:

• all business unit managers;
• [name] as Owner of the Plan and responsible for its development;
• [name] as Business Continuity Officer managing the development;
• the Recovery Team Leaders selected by the business unit managers; and
• other staff members as required from time to time.

Managers and staff must make themselves available, as they may be required, for interview in the information gathering processes.
2.9

ROLES AND RESPONSIBILITIES

Everyone involved in the development processes, and in carrying out the finished Plans, should have written, clearly defined and agreed terms of reference and responsibilities. An individual may have more than one role, provided the roles do not conflict.

2.9.1

Project Owner

The Project Owner is responsible for ensuring that:

- the fullest support for the planning project from all senior managers is obtained and maintained;
- planning activity is completed on schedule;
- there is wide awareness of the completed BCP; and
- the BCP is maintained.

2.9.2

Business Continuity Officer

A Business Continuity Officer should be appointed to be responsible for the project planning, development and review. Reporting to the Project Owner, the Business Continuity Officer:

- will organise and supervise the planning processes, the creation of the BCP and its testing, training and ongoing maintenance; and
- must have sufficient authority to ensure completion of the BCP on schedule.

The appointment should not be at so low a level that problems occur with recognising the Business Continuity Officer’s authority. Departments may decide to make this a full time duty for the development and testing period. For the subsequent training, review and maintenance it would probably be a part time duty.
2.9.3 Premises Manager

The Premises Manager is:

• responsible for:
  - the premises and its maintenance;
  - repair and refurbishment to meet the requirements of the premises users;
• a facilitator to the development of the planning process;
• **not** responsible for the recovery of the users’ operations.

Business Continuity planning involves everyone and everything in a property: although Premises Managers often act as facilitators for BCP projects, they are **not** intended to have sole responsibility for the planning of Business Continuity.

2.9.4 Business Continuity Team

The **BCT**:

• is the highest level of management in the recovery organisation;
• is responsible for deciding:
  - whether or not an incident situation exists;
  - whether or not to invoke the **BCP**; and
  - the conduct of the recovery;
• comprises all business unit management or their deputies; and
• will have a Leader and Deputy Leader.

2.9.5 Recovery Teams

Individual Recovery Teams will carry out the recovery of the critical operations. There may also be facilities or infrastructure Recovery Teams for:

• premises;
• Information Technology (IT);
• communications, including liaison with the media;
• recovery administration; and
• staff welfare.
The Recovery Teams will report to the BCT. They will consist of key people from the relevant areas and have assigned Leaders and Deputy Leaders. Leaders could be members of the BCT, provided the two roles do not conflict.
2.10 WHAT SHOULD YOU DO?

1. Involve all managers in the development project for Business Continuity Planning.

2. Establish whether your premises are at an immediate or high risk:
   a. If they are, go to section 9, The Interim Plan. Decide whether an Interim Plan is needed and take the appropriate action;
   b. If they are not, go to step 3.

3. Appoint a BCP Project Owner.

4. Appoint a Business Continuity Officer.

5. Draft the objectives and scope for the BCP project.
3.0 RISK ASSESSMENT

3.1 About this Section
3.2 What is Risk Assessment?
3.3 What is an Asset?
3.4 What is a Threat?
3.5 Risk Assessment Methods
3.6 Conducting a Risk Assessment
3.7 Risk Management
3.8 Choosing Cost-Effective Countermeasures
3.9 Learning from Experience
3.10 What Should You Do?

Annex 3/1 Risk Assessment Worksheet
3.0 RISK ASSESSMENT

3.1 ABOUT THIS SECTION

This section explains:

- what Risk Assessment is;
- how to assess the Department’s assets and identify risks to the premises and the operations carried out in it;
- Risk Assessment methods;
- how to identify cost-effective measures to prevent risks; and
- how to use Risk Management techniques to control risks.

3.1.2 Key Points

The key points to note for Risk Assessment are:

- risks must be identified and assessed before they can be managed;
- a systematic approach to Risk Assessment should be taken. Risk is assessed by:
  1. considering the:
     - asset and its value to the Department;
     - threats to the asset;
     - likelihood of the threat happening; and
     - vulnerability of the asset to the threat; and
  2. assigning appropriate values to asset cost, likelihood of the threat happening and vulnerability of the asset to the threat using an appropriate formula;
- an understanding of the type of asset under review is necessary to conduct an accurate Risk Assessment;
- Risk Management controls and reduces the overall level of risk that a Department faces;
• risks are managed by avoidance, transfer, control, and acceptance;

• countermeasures introduced to control and reduce risks should be effective, appropriate, affordable and flexible;

• after every Risk Assessment, a report should be compiled, so that the details are available when the Risk Assessment is reviewed;

• Risk Assessments should be reviewed:
  - at least every year; or
  - when there have been significant changes within the Department; or
  - if there is reason to believe the original Risk Assessment is no longer valid, for example, following an incident.
3.2 WHAT IS RISK ASSESSMENT?

Risk is exposure to unwanted loss. In terms of Business Continuity, it is the risk of an incident happening which may result in unwanted loss of an asset or delay to operations.

Risk Assessment is the systematic identification of all risks, their investigation and grading relevant to each other and to the Department, so that management can be given a clear and full understanding of the risks it faces.

Risk Assessment is an important phase in the development of a Business Continuity Plan (BCP). The aims of Risk Assessment are to:

- identify the risks that Departments face;
- identify essential operations that must be restarted as quickly as possible after a disaster has taken place;
- identify cost-effective measures that could be introduced to prevent risks or lessen their impact, thereby reducing the need for the Incident Control Team (ICT) to be mobilised; and
- provide input for Risk Management.

To the inexperienced person, Risk Assessment may appear to be very complicated. If appropriate, consideration should be given to:

- seeking advice from colleague(s) with experience in this area; or
- employing or commissioning a consultant specialising in Risk Assessment.
3.3 WHAT IS AN ASSET?

An asset is a resource, anything of value to the organisation, tangible and intangible, for example the premises, telephones, staff and their skills. A Department’s assets are likely to include, among other things, the:

• premises;
• access rights to the premises;
• staff;
• electrical system;
• IT equipment;
• telephone system;
• computer and paper-based records;
• water supply and drainage systems;
• heating and ventilation systems;
• fixtures and fittings; and
• furniture and equipment.

This list is not intended to be exhaustive, and Departments must consider what their own particular assets are.
3.4 WHAT IS A THREAT?

A threat is anything with potential for adverse effect on an asset, for example fire, unauthorised access to premises. Threats should be assessed to determine:

- how vulnerable the Department’s assets are to the threats;
- what preventative measures could be taken to lessen the impact of the threats.

The types of threat a Department’s assets may be at risk from are:

- natural threats, such as:
  - fire;
  - flood;
  - storm;
  - lightning; and
  - power failure;
- deliberate and violent threats from people, such as:
  - arson;
  - bomb;
  - sabotage; and
  - vandalism;
- deliberate and non-violent threats from people, such as:
  - theft;
  - strike; and
  - disclosure;
- accidental threats, such as:
  - outage;
  - error; and
  - disclosure.
Departments should also consider threats arising from:

- unauthorised access to:
  - the premises;
  - equipment;
  - papers and other resources; and
  - computer systems, from outside and inside the premises;

- the location of the premises, for example:
  - road, rail and air traffic;
  - industrial processes;
  - gas holders;
  - visible targets for terrorism, for example environmental, religious, political;
  - building works; and
  - planning regulations, for example changes in permitted use of neighbouring premises;

- the premises itself, for example:
  - the boundaries;
  - the surrounding land;
  - the outside of the premises; and
  - entrances and exits;

- within the premises, for example:
  - the presence of asbestos;
  - lack of protective film on windows to stop flying glass;
  - service failures which could stop work or cause staff to walk out, for example heating, lifts;
  - storage of valuable objects, such as valuable documents stored in a basement prone to flooding;
  - absence of ‘clear desk’ policy;
• shared premises. If the premises are shared with other occupants, consideration should be given as to whether they, or their activities, pose any additional threat, or weaken security. Occupants of shared premises:

- are legally required to co-operate in and co-ordinate emergency procedures and health and safety arrangements;

- should agree who is responsible for what during an emergency situation, for example boarding up broken windows, calling in electricians or plumbers; and

- should review these responsibilities on a regular basis.

**Note:** Historic Buildings may have additional or special risks because of their construction, historical value or the constraints of being listed.

### 3.4.1 Other Areas to Investigate

The table at section RISK 3.4.2 is a checklist of other considerations not specifically linked to individual assets that Departments should investigate when carrying out Risk Assessments. For each item in the **Areas for Investigation** column the question ‘Is the situation satisfactory?’ should be considered and ‘Yes’ or ‘No’ entered in the second column. The checklist can then be used to:

- create a status report; and

- identify any improvements or deterioration, if used at regular intervals.

The list is not intended to be exhaustive.

See the *Premises Management Guide* for further details on the areas listed in the table.
### Risk Assessment Checklist

<table>
<thead>
<tr>
<th>Areas for Investigation</th>
<th>Status (Yes/No/Comments)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existence of fire and other emergency evacuation procedures</td>
<td></td>
</tr>
<tr>
<td>Existence of bomb threat procedures</td>
<td></td>
</tr>
<tr>
<td>Appointment of Floor/Area Fire Wardens</td>
<td></td>
</tr>
<tr>
<td>Existence of training and testing for Floor/Area Fire Wardens</td>
<td></td>
</tr>
<tr>
<td>Reliance on telephone, fax, IT equipment</td>
<td></td>
</tr>
<tr>
<td>List of reliable contractors for emergency repairs</td>
<td></td>
</tr>
<tr>
<td>Dependency on specific goods and services</td>
<td></td>
</tr>
<tr>
<td>Dependency on specific equipment</td>
<td></td>
</tr>
<tr>
<td>Computer data backed up and stored off site</td>
<td></td>
</tr>
<tr>
<td>Compliance with legislation on public health, health and safety, fire precautions</td>
<td></td>
</tr>
<tr>
<td>Compliance with listed building constraints</td>
<td></td>
</tr>
<tr>
<td>Works of art or unique, historic or irreplaceable artefacts and documents</td>
<td></td>
</tr>
<tr>
<td>Vehicles - parking</td>
<td></td>
</tr>
<tr>
<td>Subsidence, landslip</td>
<td></td>
</tr>
<tr>
<td>Leakages, burst pipes, internal flooding - water, oil, gas</td>
<td></td>
</tr>
<tr>
<td>Power isolation devices on electrical systems</td>
<td></td>
</tr>
</tbody>
</table>
3.4.3 Countermeasures

When considering the assets and threats, countermeasures may suggest themselves. If simple and very cheap they could be applied at once, otherwise they should be carefully noted for later consideration. For example, in looking at access to the building, a seldom-used entrance could be:

- locked, which would be cheap;
- bricked up, which would be more expensive; or
- covered by closed circuit television which would be very expensive if CCTV is not already in use.

Note: fire escape routes must not be compromised by locked doors.
3.5

RISK ASSESSMENT METHODS

If Risk Management is to be effective, a systematic approach to Risk Assessment should be taken. This means that Risk Assessment should be conducted formally, rather than casually. The casual method is to walk around:

- looking for possible threats;
- asking people’s opinions;
- weighing everything up mentally; and
- giving a judgmental assessment.

The casual method will inevitably result in omissions and inconsistency.

Adopting a more formal, systematic approach will enable:

- a more thorough and consistent Risk Assessment to be carried out; and
- comparisons between risks to be made.

By comparing the risks a Department faces, they can be ranked in order of priority and the greatest risks to the Department dealt with first. To compare different risks accurately, they must all be assessed in the same way, so that the results are consistent. Similarly, assessments of the same risk carried out at different times must be consistent, so that any improvement or deterioration can be detected.

The following methods will enable a systematic and reliable Risk Assessment to be carried out:

- value ranges - see section RISK 3.5.1 for further details;
- formulae for comparing risks - see section RISK 3.5.2 for further details;
- Risk Assessment worksheet - see section RISK 3.5.4 for further details;
- computer software if suitable - see section RISK 3.5.5 for further details.
3.5.1 Value Ranges

To assist in comparison, a range of values should be set for each of the following:

- asset cost;
- likelihood of threat happening;
- vulnerability; and
- assessment of the risk.

The following ranges can be used:

- a scale of one to five; or
- Very Low, Low, Moderate, High and Very High.

A scale of one to five will produce a more accurate Risk Assessment than a scale of one to three. Ranges greater than five are usually unnecessary and should only be used if a particularly accurate Risk Assessment is required, or a greater distinction between different risks needs to be made.

Asset cost is usually expressed in terms of money, although sometimes it can be expressed in terms of significance to the Department, for example Insignificant, Low Significance, Significant, High Significance, Most Significant. Some assets, such as the price of human safety, are intangible. They should, however, be given an arbitrary value and converted to one of the suggested ranges for use in the Risk Assessment process.

3.5.2 Formulae for Comparing Risks

To produce more precise results from a Risk Assessment, a formula can be used in conjunction with the value ranges in section RISK 3.5.1 to help with comparing and prioritising risks. For example:

\[
\text{Risk} = \frac{\text{Asset Cost} + \text{Likelihood} + \text{Vulnerability}}{3}
\]

**Note:** The term ‘threat’ is represented by likelihood and the asset’s vulnerability. It is therefore not given a value and does not appear in the formula in its own right.
Dividing the sum of asset cost, likelihood and vulnerability by three to find the average value converts the answer back to the one to five value range. For convenience, the resulting score can then be translated into words to describe the risk, such as:

- 1 - Very Low;
- 2 - Low;
- 3 - Moderate;
- 4 - High;
- 5 - Very High.

**Example**

The risk of fire to a premises has been assessed and the following values awarded:

- asset cost = 5 (the property is highly valued);
- likelihood = 4 (fire is considered to be a significant threat because the property is next door to a refinery); and
- vulnerability = 3 (fire could spread rapidly because the property is constructed of timber).

Using the formula given above, the score for this particular risk is:

\[
\frac{5 + 4 + 3}{3} = 4
\]

This translates into words as 'High' risk.

The example above and the formula used are simple and should be adequate for uncomplicated Risk Assessments. Formulae for more complicated cases cannot be given in this Guide because conditions vary from one property to another, as well as from one type of asset to another.

Anyone with a sound knowledge of Risk Assessment will be able to design value ranges and formulae for specific subjects, although these will need to be tested out first before being widely used.
3.5.3

**Risk Assessment Worksheet**

A Risk Assessment worksheet should be used to record the results of the Risk Assessment. An example of a completed worksheet is given at section RISK 3.5.4.

The following list explains what information should be entered in the different columns on the worksheet:

<table>
<thead>
<tr>
<th>Subject</th>
<th>the type of assets being assessed, for example office equipment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>the date the Risk Assessment is carried out</td>
</tr>
<tr>
<td>Asset</td>
<td>a brief description of the asset being assessed</td>
</tr>
<tr>
<td>Cost</td>
<td>a value from the chosen range for cost, based on how much it would cost to repair or replace the asset, and/or how significant the asset is to the Department</td>
</tr>
<tr>
<td>Threat</td>
<td>a brief description of the threat and its source. Extra rows can be used if there is more than one threat to an asset</td>
</tr>
<tr>
<td>Likelihood</td>
<td>how often the threat is likely to arise, for example once a day, once every ten years</td>
</tr>
<tr>
<td>Rating of likelihood</td>
<td>a value from the chosen range for likelihood</td>
</tr>
<tr>
<td>Vulnerability - success</td>
<td>how likely the threat is to succeed</td>
</tr>
<tr>
<td>Vulnerability - extent</td>
<td>how much damage there is likely to be</td>
</tr>
<tr>
<td>Vulnerability - rating</td>
<td>summary of both aspects, a value from the chosen range for vulnerability</td>
</tr>
<tr>
<td>Threat summary</td>
<td>a summary of the risk for the specific asset/threat combination</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>an overall assessment of the asset, considering the values of all the threats. The overall Risk Assessment could be the average value or the worst case, depending on which is the most suitable. <strong>Note:</strong> if the average is used, an important threat may be overlooked.</td>
</tr>
</tbody>
</table>

A blank Risk Assessment worksheet which can be photocopied and used is given at Annex 3/1.
### Risk Assessment Worksheet: Example

**Subject:** Office equipment  
**Date:** 25 March 1998

Use extra lines if there is more than one threat per asset.

<table>
<thead>
<tr>
<th>Asset</th>
<th>Cost</th>
<th>Threat</th>
<th>Likelihood</th>
<th>Rating of Likelihood</th>
<th>Vulnerability</th>
<th>Threat Summary</th>
<th>Overall Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Telephone</strong></td>
<td>£50,000 (3)</td>
<td>Unauthorised access</td>
<td>Once a month</td>
<td>Low to (2-3) Moderate</td>
<td>Low (2)</td>
<td>High (4)</td>
<td>Moderate (3)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Serious breakdown</td>
<td>Once a year</td>
<td>Very Low (1)</td>
<td>Very Low (1)</td>
<td>Moderate (3)</td>
<td>Low (2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fire</td>
<td>Once in 2 years</td>
<td>Very Low (1)</td>
<td>Moderate (3)</td>
<td>High (4)</td>
<td>Moderate (3)</td>
</tr>
<tr>
<td><strong>Photocopiers</strong></td>
<td>£10,000 (1) Very Low</td>
<td>Unauthorised access</td>
<td>Once a month</td>
<td>Low to (2-3) Moderate</td>
<td>Low (2)</td>
<td>High (4)</td>
<td>Moderate (3)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Theft</td>
<td>Once a month</td>
<td>Moderate (3)</td>
<td>Moderate (3)</td>
<td>High (4)</td>
<td>High (4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Serious breakdown</td>
<td>Once in 10 years</td>
<td>Very Low (1)</td>
<td>Very Low (1)</td>
<td>Moderate (3)</td>
<td>Low (2)</td>
</tr>
<tr>
<td><strong>Furniture</strong></td>
<td>£5,000 (1) Very Low</td>
<td>Fire</td>
<td>Once in 2 years</td>
<td>Very Low (1)</td>
<td>Moderate (3)</td>
<td>High (4)</td>
<td>Moderate (3)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Theft</td>
<td>Once in 10 years</td>
<td>Very Low (1)</td>
<td>Low (2)</td>
<td>Moderate (3)</td>
<td>Moderate (3)</td>
</tr>
<tr>
<td><strong>Ming Vase</strong></td>
<td>Priceless Very High (5)</td>
<td>Theft, damage</td>
<td>Once in 10 years</td>
<td>Very Low (1)</td>
<td>High (4)</td>
<td>Very High (5)</td>
<td>Very High (5)</td>
</tr>
</tbody>
</table>
3.5.5 Computer Software

Computer software packages for Risk Assessment are available. Before a particular package is chosen, it should be examined carefully and compared with others on the market to make sure that it is the most suitable one. PACE may be able to advise staff who are considering using a software package for Risk Assessment.

It must be remembered that software is only a tool and cannot carry out Risk Assessment on its own. The user must:

- know how to operate the software properly;
- input the correct information; and
- interpret the data generated by the software correctly.
CONDUCTING A RISK ASSESSMENT

Whichever method is chosen to conduct a Risk Assessment, the premises itself, plus everything in and around it, should be considered. To make this task manageable, the Risk Assessment should be broken down into separate assessments, each covering a specific area (such as a group of assets and/or operations), for example:

- security arrangements on the premises;
- computer security;
- communications; and
- essential supplies and services.

Due to the volume of work involved, two or more people may need to conduct the separate assessments, so that the Risk Assessment is completed within a reasonable amount of time. Those responsible for gathering information should have a sound knowledge of Risk Assessments, so that they know:

- what sort of questions to ask; and
- how to interpret the answers correctly.

Information needed to conduct the Risk Assessment can be gathered by:

- interview;
- physical inspection; and
- consulting any history of previous incidents.
3.6.1 Stages of a Risk Assessment

A Risk Assessment should follow these stages:

1. All the Department’s assets should be listed, with similar assets grouped together, for example all the PCs in the premises.

2. For each asset, it should be decided:
   - how much the asset would cost to replace;
   - the value of the asset’s cost from the chosen range for cost, for example a telephone system worth £50,000 could be translated to a range value of 3; and
   - the asset’s value to the organisation, and/or the consequential loss which would arise if the asset were not available.

3. For each asset, the threats it is subject to should be listed, for example fire or breakdown.

4. For each threat:
   - the likelihood of it occurring should be determined. This is the most difficult factor to establish and is likely to be highly judgmental; and
   - a value in the range for likelihood should be awarded, for example fire: 3, breakdown: 1.

5. Each asset/threat combination should be awarded a value in the range for vulnerability, for example telephones/fire: 3, telephones/breakdown: 2, by considering:
   - if the threat occurs, how likely it is to materialise; and
   - if the threat materialises, how widespread its impact will be.

6. The potential for loss should be summarised and an assessed value awarded to the risk. (The risk at this point is to the specific asset/threat combination.) This is done by using the chosen formula or is a judgmental assessment for each threat to a given asset.

7. To complete the overall Risk Assessment of the asset, the values of all the threats to a specific asset should be considered together. The overall Risk Assessment could be the average value, or the worst case, depending on which is the most suitable.

Note: if the average value is used, an important threat may be overlooked.
3.6.2 Risk Assessment Report

After every Risk Assessment, a report should be compiled, so that the details are available when the Risk Assessment is reviewed. The report should include:

- how the Risk Assessment was carried out;
- any relevant observations made during the Risk Assessment;
- the findings and conclusions; and
- any action already taken as a result of the Risk Assessment; and
- recommendations on action that should be taken in the future.

If any of the recommendations involve policy or budget and require management approval before any action is taken, the report should be sent to the appropriate manager.
3.7 RISK MANAGEMENT

Risk Management is the process of reducing and controlling the risks that a Department faces. It is usually an established, ongoing process. The benefits of Risk Management can be expressed in financial terms and effort saved by minimising or removing the delays and losses caused by risks which would result in damage.

To manage risks effectively, Departments must:

- prioritise risks; and
- select the best method of protection against the risks.

3.7.1 Prioritising Risks

The results of the Risk Assessment will show which risks should be given priority. Departments should deal with the highest risks first, as this will have a greater effect on overall risk reduction. However, this may be time-consuming and expensive, for example installing closed circuit television (CCTV) and centrally-controlled door locks to prevent unauthorised access to the premises. Departments may, therefore, decide to deal with lower risks in parallel.

3.7.2 Types of Protection

Methods of protection against a risk must:

- be effective; and
- cost a reasonable amount compared to the asset cost and likelihood of the risk.

Methods of protection in order of preference are:

1. **Avoidance**: changes should be made to eradicate the risk completely, for example to stop using an asset or a process which affects it, or move the asset into a secure environment, such as bringing a bicycle rack inside a fence to prevent bicycles from being stolen.

2. **Transfer**: if the risk cannot be avoided, consideration should be given as to whether it can be transferred to someone else who can manage it better, ie the asset could be hired rather than owned, for example contracting out the payroll process.
3. **Control:** if the risk cannot be transferred to someone else, a control should be installed to:
- prevent the risk from materialising, for example posting a security guard at the main entrance; or
- issue an early warning, so that action can be taken as soon as possible, for example installing an intruder alarm on all windows.

4. **Acceptance:** if, after a full Risk Assessment, it is decided that a risk or asset cost is minimal, or no cost-effective countermeasures are possible, Departments may decide to accept the risk. However, it is vital that they understand fully the implications of accepting the risk. Departments often accept risks simply because they are unaware of them, or do not understand them, for example continuing to store personnel files in a boiler room.

### 3.7.3 Risk Matrix

The diagram below illustrates the appropriate form of Risk Management for different combinations of cost of damage and likelihood. Although it only shows the four most extreme cases, more moderate cases can easily be deduced from it.
3.7.4 **Review of Risk Assessments**

All Risk Assessments should be reviewed at least annually, or more frequently if there have been significant changes within the Department, or there is reason to believe the original Risk Assessment is no longer valid, for example following an incident, to determine if:

- the countermeasures are still in place and are working as expected;
- the risks have changed. If this is the case, the countermeasures taken to control the risks may have to change too;
- any new risks have appeared. New threats that appear suddenly should be assessed immediately and new or revised countermeasures selected; and
- any risks have disappeared. If this is the case, the countermeasures that were introduced to control these risks may now be redundant and removing them may save money and effort.

3.7.5 **Risk Awareness and Ownership**

Making staff aware of risks can help to identify and reduce them. Assigning ‘ownership’ of high risks to the appropriate managers delegates the responsibility for monitoring and controlling them. This can be particularly effective if the risk often materialises, for example theft.
3.8 CHOOSING COST-EFFECTIVE COUNTERMEASURES

When considering the assets and threats, there may be obvious countermeasures that Departments could consider. If simple and inexpensive, they could be applied immediately, otherwise they should be carefully noted for later consideration. For example, in looking at access to the premises, a seldom-used entrance could be:

- locked (inexpensive) (Note: Fire escape routes must not be obstructed by locked doors);
- bricked up (more expensive); or
- covered by CCTV (very expensive if CCTV is not already in use).

Countermeasures must be:

- effective - provide all the protection required;
- appropriate - suitable for the risk and the asset to be protected;
- cost-effective - appropriate to the asset cost or potential damage, and affordable;
- flexible - should remain effective even if the threats change.

Effective countermeasures to prevent a risk from materialising should become obvious when considering:

- what the asset is;
- the threat to it; and
- the source of the threat.

To find the best option, a number of alternative countermeasures should be compared and any that do not meet the above criteria rejected. For example, attaching a padlock to a garden shed door is far more appropriate than fitting a bank vault door to the shed.

It is possible that there will be no suitable countermeasures.
Departments may wish to consider using a combination of several countermeasures to produce a ‘defence in depth’, that is, a succession of obstacles a threat would have to overcome before an incident occurred. For example, to make the premises more secure:

- erect a fence with only one gate around the premises;
- install floodlights;
- install CCTV;
- have full-time security guards and electronic door locks on each floor, or area on a floor; and
- issue security passes to all staff and visitors.
LEARNING FROM EXPERIENCE

The ability to identify and assess a risk is often based on personal experience and knowledge. Advice on how to identify previously unrecognised risks, or to understand existing risks better and be equipped to protect against them can be obtained from, for example:

- colleagues;
- reports of previous Risk Assessments;
- Risk Assessment publications;
- risk organisations; and
- records of incidents which have happened in the past.
3.10 WHAT SHOULD YOU DO?

1. Seek help and advice when necessary from colleagues with experience of Risk Assessment, or by employing or commissioning a specialist consultant in this area.

2. Make a list of the assets and other areas to be assessed for the premises or operation.

3. Consider all the threats, referring to section RISK 3.4 and the checklist in section RISK 3.4.2.


5. Make sure you understand fully the subject to be assessed, seeking advice when necessary, so that you can:
   - plan the assessment; and
   - interpret the results correctly.

6. Plan how you will conduct the Risk Assessment, considering the options given in section RISK 3.5. Decide:
   - which value ranges are appropriate;
   - whether to use a formula. If so, design and test one; and
   - if the average or worst case is appropriate for the final assessment.

7. Conduct the assessment, following the steps in section RISK 3.6.

8. Record the results on a Risk Assessment worksheet.

9. Note any measures identified during the Risk Assessment that could be taken to protect an asset. At the end of the Risk Assessment, refer the measures to Risk Management for action.

10. Review the results to check they are accurate and assess what conclusions you can draw from them.

11. Compile a written report, including findings, conclusions and any recommendations for further action.

12. If any of the recommendations involve policy or budget and require management approval, send a copy of the report to the appropriate manager.

13. Introduce any cost-effective countermeasures identified during the Risk Assessment to protect assets from any threats they may be subject to.

14. Monitor the results of the Risk Assessment and set a review date.
### Annex 3/1: Risk Assessment Worksheet

**Subject:** Office equipment  
**Date:** 25 March 1998

Use extra lines if there is more than one threat per asset.

<table>
<thead>
<tr>
<th>Asset</th>
<th>Cost</th>
<th>Threat</th>
<th>Likelihood</th>
<th>Rating of Likelihood</th>
<th>Vulnerability</th>
<th>Threat Summary</th>
<th>Overall Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4.0 BUSINESS IMPACT REVIEWS

4.1 ABOUT THIS SECTION
4.2 BUSINESS IMPACT REVIEW INTERVIEWS
4.3 COMPARING THE IMPACT OF OPERATION STOPPAGES
4.4 ASSESSING THE IMPACT OF OPERATION STOPPAGES
4.5 IDENTIFYING ESSENTIAL OPERATIONS
4.6 BUSINESS IMPACT REVIEW REPORT
4.7 WHAT SHOULD YOU DO?

ANNEX 4/1 BUSINESS IMPACT REVIEW - INTERVIEW WORKSHEET
ANNEX 4/2 BUSINESS IMPACT REVIEW - IMPACT WORKSHEET
ANNEX 4/3 BUSINESS IMPACT REVIEW - OPERATION SUMMARY WORKSHEET
4.0 BUSINESS IMPACT REVIEWS

4.1 ABOUT THIS SECTION

This section explains how:

- Business Impact Review (BIR) interviews are conducted to:
  - identify the essential operations which need to restart as soon as possible after a disaster has occurred;
  - establish how soon the essential operations must restart after a disaster has occurred; and
  - identify the minimum resources needed for the essential operations to restart;
- to summarise the impact of operation stoppages;
- to assess the severity of the impact; and
- to write BIR reports.

4.1.1 Key Points

The key points to note for BIRs are:

- before essential operations can be identified, BIR interviews should be conducted to identify all the operations carried out in the premises, using the BIR Interview Worksheet for guidance;
- BIR interviews should be:
  - conducted in person rather than by telephone;
  - arranged in advance with the managers of the various business units, ensuring that all interviewees are fully briefed on what to expect; and
  - well planned so that the right information is obtained without wasting time;
• information obtained from BIR interviews should be recorded on BIR Interview Worksheets, so that all results are recorded in a consistent way;

• all BIR Interview Worksheets should be compared to check whether the impact of an operation stoppage appears in more than one place. Any discrepancies should be resolved with the interviewees;

• information recorded on BIR Interview Worksheets should be copied onto Impact Worksheets;

• all operations should be assessed to establish:

  - what the impact on other operations and business units would be if they stopped; and

  - how severe the impact of the operation stoppage would be, taking into account the impact and the Maximum Acceptable Outage Time (MAOT);

• all impacts should be listed on Operation Summary Worksheets under their operations in descending order of severity;

• all the main operations carried out on the premises should be assessed to establish whether they are essential. Essential operations are operations that must restart as quickly as possible after a disaster has occurred;

• a report summarising the results of BIRs should be written and circulated to all Departments in the premises for approval of the conclusions.
4.2 BUSINESS IMPACT REVIEW INTERVIEWS

Before essential operations can be identified, it is necessary to identify all the operations carried out in the premises. This information can be obtained by interviewing the heads of business units.

BIR interviews can be carried out:

- in person, whenever possible; or
- by telephone, in unavoidable situations.

Personal BIR interviews are preferable as they:

- hold the interviewee’s attention for longer; and
- allow the interviewer to:
  - ask supplementary questions; and
  - follow up other leads which may appear in the course of the interview.

The telephone should only be used for BIR interviews to:

- clarify information obtained from a personal interview; or
- ask follow-up questions which can be answered in a few minutes.

4.2.1 Preparing for Business Impact Review Interviews

When arranging BIR interviews, the following points should be considered:

- all interviews should be arranged in advance with the heads of the various business units;
- all interviewees should be briefed on what to expect, so that they can prepare for the interview and provide relevant information;
- all interviews should be well planned; and
- if the interviews are delegated, the interviewers also need careful briefing, to be given a clear understanding of what is required.
4.2.2

Business Impact Review Interview Checklist

The following checklist can be used as an aide-memoire during BIR interviews. The list is not exhaustive because interviews are exploratory in nature and can be unpredictable. Instead, it lists the basic questions that should be asked. The quality of the interview depends on the interviewer’s ability to recognise and follow up important leads which appear in the course of the interview.

**Checklist**

1. What are the major operations carried out on the premises?

2. For each major operation:
   a. Does it depend on the availability of a product or service from outside the business unit or premises?
      - If yes, what is the effect if the product or service is unavailable?
      - Does the interviewee have any control over the availability of the product or service?
      - How long can the operation continue without the product or service?
   b. Who depends on the products of this operation?
      - How are they affected if the product or service is unavailable?
   c. Are there any legal, contractual, statutory, social or political obligations to carry out the operation?
      - If yes, what are they?
      - What are the implications of an operation stoppage?
      - How long can the operation stoppage last before it becomes unacceptable?

3. Are there any forthcoming changes which will have implications on the operation?
   If yes, what are they?

4. What are the minimum resource requirements to enable the interviewee’s business unit to recover from an operation stoppage, for example:
   a. number of staff after 1 day, 5 days, 10 days etc;
   b. number of desks, chairs, telephones, PCs;
   c. any special equipment; and
   d. any other resources needed (apart from the usual stationery and photocopiers).
4.2.3 **Interview Worksheet**

Information obtained from BIR interviews should be recorded on an Interview Worksheet. This ensures that the results of all interviews are recorded in a consistent way. A blank sample Worksheet is given at Annex 4/1 to this section.

An example of a completed BIR Interview Worksheet is shown at section BIR 4.2.4. The following information should be entered in each column of the worksheet. More than one row should be used if several entries need to be made under the same category.

<table>
<thead>
<tr>
<th><strong>Operation</strong></th>
<th>name or brief description of the operation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input</strong></td>
<td>name or brief description of critical input needed for the operation to be carried out</td>
</tr>
<tr>
<td><strong>Input Source</strong></td>
<td>from where the critical input comes</td>
</tr>
<tr>
<td><strong>Outage Time</strong></td>
<td>how long the operation can continue without the critical input</td>
</tr>
<tr>
<td><strong>Control</strong></td>
<td>how much control over the input there is, for example none, poor, total, contractual</td>
</tr>
<tr>
<td><strong>Output</strong></td>
<td>name or brief description of the product or service resulting from the operation</td>
</tr>
<tr>
<td><strong>Recipient</strong></td>
<td>who needs the output (to be followed up with recipient)</td>
</tr>
<tr>
<td><strong>Obligations</strong></td>
<td>details of any legal, contractual, statutory, social or political obligations to carry out the operation</td>
</tr>
<tr>
<td><strong>Impact</strong></td>
<td>brief description of the impact of an operation stoppage, severity and who will be affected</td>
</tr>
<tr>
<td><strong>Criticality</strong></td>
<td>how quickly the operation must be resumed after a disaster has occurred, as perceived at the time of the interview. May be updated as the interviews proceed</td>
</tr>
<tr>
<td><strong>Comment</strong></td>
<td>brief comment from the interviewer and interviewee, as appropriate, to cover, for example, details of forthcoming changes which may affect the operation</td>
</tr>
</tbody>
</table>
### Business Impact Review - Interview Worksheet - Example

<table>
<thead>
<tr>
<th>Name of Interviewee:</th>
<th>Department/Business unit:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interviewer:</td>
<td>Date:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operation</th>
<th>Input</th>
<th>Input Source</th>
<th>Outage Time</th>
<th>Control</th>
<th>Output</th>
<th>Recipient</th>
<th>Obligations</th>
<th>Impact</th>
<th>Criticality</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Building Security</td>
<td>Guards present</td>
<td>Staff</td>
<td>1 hour</td>
<td>Total</td>
<td>Access control</td>
<td>All in premises</td>
<td>Political</td>
<td>Open access</td>
<td>Very High</td>
<td>Essential to control access to building</td>
</tr>
<tr>
<td>CCTV</td>
<td>owned</td>
<td>Service contract</td>
<td>1 hour</td>
<td>Access control</td>
<td>All in premises</td>
<td>Reduced control</td>
<td>High</td>
<td>Essential</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Locks to floors</td>
<td>owned</td>
<td>Service contract</td>
<td>24 hours</td>
<td>Access control</td>
<td>All on floor(s)</td>
<td>Reduced control</td>
<td>High</td>
<td>Essential</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Payroll Systems</td>
<td>Computer system</td>
<td>Computing</td>
<td>1 day</td>
<td>None</td>
<td>Monthly pay</td>
<td>All staff</td>
<td>Contractual, Social</td>
<td>Staff unpaid</td>
<td>High</td>
<td>Very important in last week of month</td>
</tr>
<tr>
<td>Starters, leavers</td>
<td>Personnel</td>
<td>None</td>
<td>4 days</td>
<td>Ditto</td>
<td>Affected staff</td>
<td>Ditto</td>
<td>Payment errors</td>
<td>High</td>
<td>Ditto</td>
<td></td>
</tr>
<tr>
<td>Overtime</td>
<td>Business units</td>
<td>None</td>
<td>1 week</td>
<td>Ditto</td>
<td>Ditto</td>
<td>Ditto</td>
<td>Unpaid overtime</td>
<td>Moderate</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Edition 1: May 1998
4.3 COMPARING THE IMPACT OF OPERATION STOPPAGES

When all the necessary BIR interviews have been completed, all BIR Interview Worksheets should be compared to check whether the same impact of an operation stoppage occurs in more than one place. Any discrepancies in the severity of the impact (see the Impact column) or outage time (see the Outage Time column) must be resolved with the interviewees.

4.3.1 Impact Worksheet

Information recorded on the Interview Worksheets should be copied onto an Impact Worksheet. A blank sample Impact Worksheet is given at Annex 4/2.

An example of a completed Impact Worksheet is given at section BIR 4.3.2. The following information should be entered in each column of the Worksheet:

- **Impact - name or brief description**: brief description of the impact of an operation stoppage
- **Source of impact**: operation or business unit causing the impact (may be external)
- **Subject of impact**: operation or business unit subject to the impact
- **Maximum Acceptable Outage Time - to subject of impact**: highlight the shortest time if there is more than one
- **Effect - fuller description**: fuller description of the impact of the operation stoppage
- **Consequence - if uncorrected, Obligation**: what will happen if the impact is not corrected. Will any obligations to other business units be affected?
- **Assessed Severity**: assessment of how severe the impact of the operation stoppage would be, using the agreed classification categories and ranges.
### Business Impact Review - Impact Worksheet - Example

<table>
<thead>
<tr>
<th>Prepared by:</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Impact - name or brief description</strong></td>
<td><strong>Source of impact</strong></td>
</tr>
<tr>
<td>Lack of Security Guards</td>
<td>Illness</td>
</tr>
<tr>
<td>CCTV failure</td>
<td>Breakdown</td>
</tr>
<tr>
<td>Floor door lock failure</td>
<td>Breakdown</td>
</tr>
<tr>
<td>Loss of Payroll system</td>
<td>Computer failure</td>
</tr>
<tr>
<td>Loss of payroll input, starters/leavers</td>
<td>Personnel</td>
</tr>
<tr>
<td>Loss of overtime input</td>
<td>Business units</td>
</tr>
</tbody>
</table>
4.4 ASSESSING THE IMPACT OF OPERATION STOPPAGES

When all details have been entered on the Impact Worksheet, all operations should be assessed to establish:

- what the impact on other operations and business units would be if they stopped; and
- how severe the impact of the operation stoppage would be.

The following factors should be taken into account when assessing how severe the impact of operation stoppages is:

- the impact itself; and
- the MAOT.

4.4.1 Impact Categories

A decision needs to be taken on whether the impact of operation stoppages needs to be quantified in detail. For most BIRs, simple classification categories for impact are usually adequate, for example:

- Very Low;
- Low;
- Moderate;
- High; and
- Severe.

However, if it is difficult to agree on the conclusions from a BIR, it may be necessary to use a more complex method, for example expressing impact in terms of financial loss, which would require substantial planning and effort to validate the results.

4.4.2 Maximum Acceptable Outage Time

The MAOT is usually used to assess the severity of the impact of an operation stoppage and is the maximum length of time an operation stoppage can last before the impact becomes unacceptable or affects other operations.
A suitable range for assessing MAOTs should be chosen, for example 1 day, 5 days, 10 days, more than 10 days. Three time ranges should be sufficient for most BCPs. Different business units may wish to use different timescales, for example the time to update medical records may be classified by a hospital’s Casualty Unit in minutes and its Records Unit in days. This will mean that their answers will need to be rationalised.

4.4.3 Operation Summary Worksheet

When the severity of each impact has been assessed, an Operation Summary Worksheet should be completed, listing all impacts under their operations in descending order of severity. A blank sample Operation Summary Worksheet is given at Annex 4/3 to this section. Criticality Assessments should be made by summarising the Impacts and MAOTs.

An example of a completed Operation Summary Worksheet is given at section BIR 4.4.4. The following information should be entered in each column of the worksheet:

- **Operation**: name or brief description of the operation subjected to the impact
- **Impact**: brief description of the impact of an operation stoppage
- **Severity of impact**: an assessment of the impact using the agreed classification categories and ranges
- **Maximum Acceptable Outage Time**: (to the subject of the impact). The shortest time, if there is more than one, needs to be highlighted
- **Criticality Assessment of Operation**: an assessment of how important the operation is, taking all the impacts and MAOTs into account, using the agreed scale
- **Comment**: any further information, for example whether the source is external and where it is.
### Business Impact Review - Operation Summary Worksheet - Example

**Department:**

**Prepared by:**

**Date:**

Use extra lines if there is more than one Impact per Operation.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Impact</th>
<th>Severity of Impact</th>
<th>Maximum Acceptable Outage Time</th>
<th>Criticality Assessment of Operation</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Too many guards absent</td>
<td>Very High</td>
<td>1 hour</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Loss of CCTV</td>
<td>High</td>
<td>1 hour</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Floor door lock failure</td>
<td>High</td>
<td>1 day</td>
<td>Very High</td>
<td>Good security essential</td>
<td></td>
</tr>
<tr>
<td>Payroll</td>
<td>Computer failure</td>
<td>High</td>
<td>1 day</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>No starter/leaver input</td>
<td>Moderate</td>
<td>4 days</td>
<td>Staff must be paid on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No overtime input</td>
<td>Moderate</td>
<td>1 week</td>
<td>High</td>
<td>time and correctly</td>
</tr>
</tbody>
</table>
IDENTIFYING ESSENTIAL OPERATIONS

When the Operation Summary Worksheet has been completed, all operations should be assessed to establish whether they are essential.

Essential operations are those which must restart as quickly as possible after a disaster has occurred, that is those with criticality assessed as ‘Low’ and ‘Very Low’ with correspondingly low MAOTs. Operations with stoppage impacts classed as ‘Very Low’ are usually of no real concern, although they may be included if a more comprehensive BIR is required.

When identifying essential operations, it is important to look at the right level of operation. Too low a level results in excess detail and wastes time, so it is important to concentrate on the main operations. These are usually those operations which have a greater impact if they stop, or their performance is reduced. For example, when considering the protection of premises against intruders, the operation of ‘Security Guard’ would be the right level to consider; ‘signing in visitors’ or ‘watching Closed Circuit Television (CCTV) screens’ would not.

The following are some of the operations Departments should consider when identifying essential operations:

- security;
- safety inspections;
- health and safety at work;
- building maintenance;
- equipment maintenance;
- emergency call out of electricians, etc;
- transport; and
- post collection and delivery.
To determine how important an operation is, the following factors should be considered:

- how great an impact it will have if it stops;

- the length of the MAOT, for example if stopping an operation for more than 48 hours is not acceptable, the operation is likely to be essential. If different MAOTs apply to one impact, the shortest time should be considered;

- the dependency of the operation on other operations and business units, for example payroll operation depends on the Personnel Unit to provide details of starters, leavers and salary changes. An operation itself may not be essential, but it could be essential to another operation which depends on it;

- Risk Assessment reports. These can also be used to validate the conclusions from BIRs;

- whether any forthcoming changes will increase, reduce or remove impacts, or create new ones; and

- the location of the premises. The need to be in the present location, or the security implications of being in the present location, may be very significant and could affect the:
  - impact;
  - MAOT; and
  - choice of alternative premises.
BUSINESS IMPACT REVIEW REPORT

A report summarising the results of all BIRs should be written and circulated to all Heads of business units in the premises for approval of the conclusions. This will raise their level of awareness of the development of the BCP and encourage their participation and assistance.

The report should:

• present the essential operations and their stoppage impacts, grouped in ascending order of MAOT;

• highlight impacts caused by non-performance of external suppliers;

• state the minimum resource requirements for recovery of each business unit;

• highlight the implications of any forthcoming changes on recovery; and

• support its conclusions by discussing briefly each of the major items in the report.
4.7 WHAT SHOULD YOU DO?

1. Arrange your BIR interviews in advance with the heads of the various business units and brief the interviewees on what to expect.

2. Plan your BIR interviews carefully and brief anyone assisting you, so that they understand what is required both of interviewees and themselves.

3. Base your BIR interviews on the BIR Interview Checklist given in section BIR 4.2.2.

4. Record the results of each BIR interview on separate BIR Interview Worksheets.

5. When you have completed all the necessary BIR interviews, compare all the BIR Interview Worksheets to check whether any impact occurs in more than one place. Resolve any discrepancies in the severity of the impact (see the Impact column) or outage time (see the Outage Time column) with the interviewees.

6. Transfer the information from the BIR Interview Worksheets to Impact Worksheets.

7. Decide on suitable classification categories for the impact of operation stoppages and ranges for MAOTs.

8. Assess all operations, using your chosen classification categories and ranges, to establish:
   - the impact on other operations and business units if they stopped; and
   - the severity of the impact of the operation stoppages.

9. List all impacts on Operation Summary Worksheets under their operations in descending order of severity.

10. Assess how important each operation is, ie how quickly it must restart after an incident.

11. Write a report summarising the results of the BIR and circulate it to all the Heads of business units on the premises for approval of the conclusions.

12. Take specialist advice as necessary.
## Annex 4/1: Business Impact Review - Interview Worksheet

### Name of interviewee:  
### Department:  
### Interviewer:  
### Date:  

<table>
<thead>
<tr>
<th>Operation</th>
<th>Input Source</th>
<th>Input Time</th>
<th>Outage</th>
<th>Control</th>
<th>Output</th>
<th>Recipient</th>
<th>Obligations</th>
<th>Impact</th>
<th>Criticality</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### ANNEX 4/1: INTERVIEW WORKSHEET

**BUSINESS IMPACT REVIEWS**

**Prepared by:** | **Date:**
---|---

<table>
<thead>
<tr>
<th>Impact - name or brief description</th>
<th>Source of impact</th>
<th>Subject of impact</th>
<th>Maximum Acceptable Outage Time - to subject</th>
<th>Effect - fuller description</th>
<th>Consequence - if uncorrected, Obligation</th>
<th>Assessed Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*BC/FG Edition 1: May 1998*
### Annex 4/3: Business Impact Review - Operation Summary Worksheet

Use extra lines if there is more than one Impact per Operation.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Impact</th>
<th>Severity of Impact</th>
<th>Maximum Acceptable Outage Time</th>
<th>Criticality Assessment of Operation</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.0 CONTINGENCY CONSIDERATIONS

5.1 About this Section
5.2 Use of Contingencies
5.3 Types of Contingencies
5.4 Identifying Minimum Requirements
5.5 Considering Suitable Contingencies
5.6 Evaluating and Choosing Suitable Contingencies
5.7 What Should You Do?
5.0 CONTINGENCY CONSIDERATIONS

5.1 ABOUT THIS SECTION

This section:

• discusses various contingency options and their advantages and disadvantages; and

• explains how to consider, evaluate and select suitable contingencies for inclusion in the Business Continuity Plan (BCP).

5.1.1 Key Points

The key points to note for contingency considerations are that a contingency:

• is a planned substitute for a resource which suddenly becomes unavailable;

• is more likely to be unavailable when needed if it costs less, and vice versa;

• can be a service, a facility or a procedure;

• is more likely to be reliable and easier to test if contracted from a supplier or owned by the Department;

• must fit the Business Continuity requirements of the whole business and all its operations; and

• must be suitable for its purpose.
5.2 USE OF CONTINGENCIES

A contingency is a planned substitute for a resource which suddenly becomes unavailable. Examples of contingencies a Department may need if a disaster occurs are:

- space for staff, with facilities. Specialised requirements for display and research such as the public rooms of a museum, or for warehousing, may also be needed;
- use of a mainframe computer, a set of PCs or PCs linked in a Local Area Network;
- use of a telephone switchboard or other communication facilities; and
- use of an alternative supplier for services or goods.

If a disaster occurs, a combination of contingencies is likely to be needed. The Business Impact Review (BIR) will indicate areas where the impact of a loss of resources would be unacceptably high: contingencies must be in place to make sure this does not happen.

A contingency needs to be:

- available for use within the acceptable start up time;
- able to support the minimum level of the operation for which it is required; and
- within a reasonable travelling distance, even if this is less convenient than the usual one.

5.2.1 Co-ordination of Contingencies

The selection and application of contingencies must be co-ordinated across the whole of the premises in order to meet the differing minimum requirements of all business units. The report of the BIR will identify these.
For example, the IT Department of a Government Agency which covers all of its operational costs by selling training courses to Government Departments and the general public had a contingency acquisition Plan which would restore their computing services in three weeks after a major incident in their computer room, and believed this to be adequate. However, the marketing Department considered that if the IT capability was unavailable for more than two days, training may not be able to be delivered and a significant share of their market would be lost irretrievably to competitors.

5.2.2 Availability of Contingencies

A contingency must be readily available when required. As a general rule, if there are alternatives, less expensive contingencies are more unlikely to be available when required.

It is possible to seek contingencies at the time of a disaster; particularly if it is a minor one which occurs during the normal course of business. For example, if a delivery van is temporarily off the road, a replacement can be hired for a limited period easily and inexpensively. It would not be necessary to buy and keep a spare van only for use in emergencies.

This would not apply, however, to a specialist vehicle such as a refrigerated van if sizeable losses would be incurred without it. In this case, it would be advisable to have a contract in place for the supply of a replacement vehicle.

5.2.3 Suitability of Contingencies

The contingency must also be suitable for its purpose. It would be inappropriate, for example, to relocate a museum to a warehouse other than for temporary housing of the artefacts.

However, it should be remembered that contingencies chosen for recovery will be the most suitable currently available when needed, and not necessarily the same items or services as were used before the incident.
5.3 TYPES OF CONTINGENCIES

A contingency could be:

- a service, for example photocopying;
- a facility, for example fully equipped office space; or
- a procedure, for example processing of work by a bureau.

The major contingencies Departments will need to consider are:

- alternative premises;
- office computer equipment such as PCs, photocopiers, binding machines, and backup data;
- specialist equipment, such as central computing facilities;
- furniture;
- documents and stationery;
- communications services; and
- transport/delivery services.

5.3.1 Alternative Premises

Alternative premises will often be needed following a disaster. PACE maintains:

- information on vacant properties on the Government’s Civil Estate;
- a database of all property on this Estate;
- a record of all forthcoming property events; and
- a good knowledge of the property market and suitable properties, for certain locations.

Departments may consult PACE as the information it holds and the knowledge it has may offer a low-cost option for alternative premises. If this option is decided upon, PACE will need to be informed of the amount of space required in cubic metres at the rate of 11 cubic metres per person (or the current rate specified by the Workplace (Health and Safety and Welfare) Regulations 1992).
When considering alternative premises, the following questions should be asked:

- how long will it take to find suitable premises?
- how quickly can a contract be arranged, and will the contract be suitable?
- what preparation will the new premises need, for example the installation of network cabling? (Note: Specialist suppliers/ installers of emergency computer cabling are readily available.)
- what is the current planning use of the premises and will consultation with the local planning authority be needed if the use changes?

When examining alternative premises for suitability, Departments may find it useful to assess them against a list of basic criteria, such as:

- location;
- floor space required;
- toilet facilities;
- drinking water;
- Health and Safety requirements;
- number and position of power points;
- lighting;
- cabling for voice communication and computers;
- planning use requirements; and
- access.

If a car park or other vacant land is available, portable buildings could be used as alternative premises. They may need:

- power supplies for heating and lighting;
- cables for computer and telephone connections;
- toilet facilities.

The local planning authority should be consulted about any such proposed uses as Circular 18/84 procedures may be involved and the permission of the owner of the car park or land may also have to be obtained.
If the Department’s main business operation is serving the community, then it must remain within easy access of that community. If the premises are on a ‘campus site’ it may be possible to use another property on the same site or to install portable buildings on vacant space.

### 5.3.2 Reciprocal Agreements

Agreements may be entered into with other premises and organisations for reciprocal recovery so that if one site is affected, the facilities of the other can be used for recovery. When looking for other suitable organisations, consider those involved in similar operations, for example, Magistrates’ Courts could reciprocate with Crown Courts.

Under reciprocal agreements, Departments have an implied obligation to help one another, but care must be taken to ensure that the impact of an incident does not also relocate with the affected Department to the alternative premises. For example, unless there is adequate spare capacity, the staff in the alternative premises would also be disrupted.

Meeting rooms and canteens are obvious sources of space, and working double shifts could be a practical way of reducing the impact. However, space for staff is often not the main consideration following a disaster; but rather the availability of the facilities they need within the premises such as computers and telephones. All these factors must be considered.

A reciprocal agreement is a low cost option but it must be carefully examined and agreed by the participating premises. It can be difficult to test an arrangement of this type and the ability of both parties to maintain the agreement could also change over time. Regular reviews should be undertaken.

### 5.3.3 Contracted Facilities

The only certain way to ensure that a contingency will be available is to contract for it or to own it. For example, it is possible to stockpile replacement computer equipment but this would incur additional purchase and maintenance costs. It may be more cost-effective to take out a contract with a specialist supplier for the use of specified facilities following a disaster; for example:

- portable buildings;
- computer hardware, either in the alternative premises or its own trailer accommodation; or
- installation of electrical and computer cabling.
The above examples might only be ready for use after a few days. If similar facilities are needed within a shorter time, there are specialist suppliers who offer annual contracts for the supply of computing and office services at one location. Fees vary according to the facilities required. This option will provide a cost-effective, speedy and above all reliable solution. However, possible drawbacks are:

- the location of the facilities;
- the resulting need to transport staff to the new location; and
- the ongoing annual cost.

The time restriction on the use of the facilities also needs to be considered. Suppliers will restrict the use of the contingency to a specific period which they consider long enough to resolve the problem which led to the need for the contingency. Once this period has elapsed, the user of the facility must vacate it.

Suppliers must demonstrate a depth of planning similar to the level of preparatory work invested in the BCP. A contract with a supplier should:

- state exactly what will be provided at the time of a disaster; and
- include opportunities to test on an annual basis to confirm that all items and facilities are available as stated and will support the desired recovery.

5.3.4 Owned Facilities

Acquiring a facility for sole use when required offers the least risk. For example, Departments could obtain and equip premises specifically for emergencies, either alone or with other Departments. The premises can then be designed specifically to meet current recovery requirements, and amended if these requirements change. Testing can be carried out as required and the availability of the contingency is assured.
This may be the ideal solution for some Departments, as it will meet all the recovery requirements. However, it is also by far the most expensive, and can only be justified if an immediate, guaranteed recovery is essential and requires facilities which are not readily obtainable. For example:

- in the commercial sector, financial dealing facilities, whose recovery timescales could be measured in hours; and
- NASA’s Manned Mission Control Centre, which has an exact duplicate in another building, which is up and running and ready to take over at a moment’s notice.

### 5.3.5 Computer Equipment and Services

IT requirements need careful consideration. Simple office PC systems can often be ordered from the usual supplier when needed. If this approach is used, periodic checks of suppliers’ stock status should also be made. Larger systems which require special features or configurations will need their own contingency.

If a computer contingency Plan already exists it may need to be changed to meet the needs of its users, not only its operators. That is, computing services need to be restored to the extent and within the time required by their users to recover the business unit’s essential operations.

Similar solutions and considerations apply as for premises. The recommended solution is a combined contract with one supplier for the provision of emergency computing services and office space and facilities under one roof.

### 5.3.6 Backup Data

All computer (including PC) software and data should be backed up at regular and reasonable intervals. Data stored on disks which are kept near PCs is particularly vulnerable, so backed-up data should be stored safely away from the premises. If a disaster occurs, the backup data will need to be delivered to the recovery location to enable computing services to be used, and returned to safe storage after use in recovery. Procedures for this should be part of the contingency.
5.3.7 **Furniture**

HM Treasury’s Procurement Practice and Development Division, formerly known as the Central Unit of Purchasing, holds a register of surplus furniture and equipment. However, an arrangement of this kind depends on availability at the time, and can only be tested by making periodic enquiries about availability.

5.3.8 **Documents and Stationery**

Many organisations have a high dependency on paperwork which is irreplaceable and vulnerable. Risk Management should already have put preventative measures into place, such as a ‘Clear Desk Policy’, or overnight storage in fire resistant cabinets. Departments should also consider changing their working practices so that they do not rely so heavily on paper records, for example by:

- destroying paper records that are no longer needed; or
- transferring paper records onto disk or microfilm.

Inevitably, it will be necessary to keep some paper records. When considering contingencies for these, priority should be given to any vulnerable or critically necessary items.

Documents which may need to be considered in any contingency provision would include:

- the Departmental Business Plan;
- the Department’s Mission Statement;
- Personnel records;
- the Fire Certificate for the premises;
- the Department’s Health and Safety Policy Statement; and
- other reference documents and stationery in frequent use.

Copies of documents could be stored off-site, and will need to be collected and delivered to the recovery location if a disaster occurs.
A Recovery Box could be created and kept off-site or in the Incident Control Room, containing:

- a supply of essential forms and other stationery which cannot be readily obtained;
- reference manuals; and
- other items for use in recovery.

The inclusion of items which change frequently, or even from time to time, should be avoided, unless they are considered an essential requirement. This is in order to minimise the need to keep updating the contents.

5.3.9 Other Resources

If other resources such as specialist books or equipment cannot be readily obtained at the time of a disaster, one solution could be to buy them in advance and store them in a safe place until needed. However, this could be expensive if they become obsolete over a short time scale. Another solution could be to create and maintain a list of possible suppliers, and of other users who may each be able to lend small quantities, could be created and maintained.

5.3.10 Petty Cash and Spending Authority

During the recovery, teams may need to buy urgent essential items. As normal methods of acquisition and payment will not be operating, consideration should be given to setting up a petty cash facility for the BCT. Management should consider setting financial and spending delegations.

5.3.11 Salvage

Salvage of papers, documents, other records and equipment may be possible. There are firms of salvage experts who can rescue items, stabilise their condition to prevent deterioration, and restore them to working order, if required. A contract can be arranged in advance for such a firm to respond immediately, or details of several can be held in the BCP.
5.4 IDENTIFYING MINIMUM REQUIREMENTS

During the contingency evaluation phase it should always be remembered that it is a contingency which is being considered, that is, a temporary measure to be used only until full facilities are available again. For this reason, it is necessary to identify the minimum requirements the contingencies need to support in order to achieve recovery, using the findings of the Business Impact Review report. Usually these requirements would involve significantly less than the normal full staffing level.
CONSIDERING SUITABLE CONTINGENCIES

In addition to those already discussed, the following factors should be considered when selecting suitable contingencies. Not all of the factors will apply. Unusual circumstances or operations may dictate additional or different ones. All the factors need to be weighed against the requirements for recovery identified in the Business Impact Review.

The following factors should be considered:

- the suitability of the contingency for its purpose. This is the most important consideration: if the contingency is not suitable, there is little point in continuing to consider it;

- the availability of the contingency:
  - certainty of availability - what happens if the contract to supply a contingency is not fulfilled?
  - hours and days of availability, for example, 9 am to 5 pm, Monday to Friday; and
  - time limit on availability, for example, 60 days;

- maintenance or support of the contingency, for example, a breakdown or repair facility;

- speed of access to, or delivery of, the contingency;

- speed of recovery using the contingency;

- certainty of recovery using the contingency;

- level of support for the minimum resources required;

- type of cost - one off, ongoing, during use only, or a combination;

- location - fixed or delivered to the usual premises or alternative premises;

- distance to contingency premises - from home and from other business locations;

- risks arising from an alternative location;

- legal obligations and liabilities arising from the contingency;

- the need for consultation with the local planning authority;
• other resources needed to make the contingency usable, for example, power for portable structures; and

• advantages and disadvantages of the contingency.

This list is not intended to be exhaustive.
5.6 EVALUATING AND CHOOSING SUITABLE CONTINGENCIES

If there is more than one contingency which satisfies the basic criteria, further investigation may be necessary before a final choice can be made. The basis for this choice should first be decided, for example:

• convenience;
• best service;
• best value for money; or
• a combination of all factors.

If values are then assigned to the deciding factors in a list of points for and against, it should be possible to select one contingency over the other(s). In order to allow the Recovery Strategy phase some flexibility in its deliberations, it may be advisable to offer alternative contingencies for each need. All the practical alternatives should therefore be put forward for consideration, together with any appropriate recommendations.

The choice of contingency depends on the minimum recovery requirements of all the business units which could be affected by an incident. As these requirements may change over time, all contingencies selected for use in the Recovery Strategy must be monitored and reviewed to ensure that they continue to remain effective and viable.

When suitable contingencies have been identified they should be listed and presented as input to the Recovery Strategy phase. Contracts or purchases should not be undertaken until the particular strategy for the BCP has been chosen.
5.7 **WHAT SHOULD YOU DO?**

1. From the Business Impact Review report, list:
   - the resources for which contingencies are needed; and
   - their users.

2. With the users, decide the minimum requirements for each contingency.

3. Obtain information about sources for the contingencies.

4. Consult the sources for details about the contingencies they can supply, for example:
   - cost;
   - speed and certainty of availability;
   - how they would be obtained;
   - hours of availability; and
   - limitations.

   **At this stage make no commitments with suppliers.**

5. Consider the suppliers’ answers against the minimum requirements and select or reject each contingency accordingly.

6. Record the selected contingencies and their details.

7. Monitor and review the contingencies selected for use in the Recovery Strategy to ensure that they remain effective and viable.

8. Take advice from specialist consultants.

9. Consult PACE.
6.0 RECOVERY STRATEGY

6.1 About This Section
6.2 Main Sources of Information
6.3 Identifying Alternative Strategies
6.4 Compiling a Cost-Effective Recovery Strategy
6.5 The People Factor
6.6 Recovery Strategy Report and Management Decision
6.7 Implementing the Strategy
6.8 What Should You Do?
6.0 RECOVERY STRATEGY

6.1 ABOUT THIS SECTION

This section explains how:

- alternative strategies for recovery of operations may be compared, which vary in:
  - timescales;
  - certainty of recovery; and/or
  - cost;
- to identify the most appropriate and cost-effective strategy for the recovery of essential operations as the basis for the Business Continuity Plan (BCP).

6.1.1 Key Points

The key points to note for any recovery strategy are:

- the information sources for the Recovery Strategy are the:
  - Business Impact Review (BIR) report;
  - Contingency Considerations report; and
  - business unit managers;
- ideally, three to five alternative strategies should be identified;
- each strategy should be a complete or near complete solution in itself;
- rising cost is usually directly proportional to the speed and certainty of recovery;
- the final choice or approval of a strategy rests with senior management; and
- Treasury approval should be sought for additional expenditure beyond approved Departmental allocations, if appropriate.
6.2 MAIN SOURCES OF INFORMATION

The two main sources of information for the development of a Recovery Strategy are the BIR and the Contingency Considerations reports.

The BIR will have identified the Department’s essential business operations and their minimum recovery levels and times. These are the targets which the Recovery Strategy must meet. The BIR should also have identified the implications of forthcoming planned changes which should be taken into account to make sure the chosen strategy remains relevant without additional cost.

The BIR must contain all the following information:

- the number of people to be accommodated after an incident;
- whether they must all be in the same premises;
- operations which need to be close to each other;
- special space and location needs;
- resource requirements:
  - office equipment and furniture;
  - specialist equipment;
  - computing services;
  - communication services; and
  - transport/delivery services; and
- forthcoming changes.

The Contingency Considerations report will have suggested some contingencies which could be used. These may need to be expanded or combined to provide complete solutions.

Departmental policy may influence the final choice of recovery strategy. Guidance should be obtained from senior management if policy is not clear or already understood, so that it may be taken into consideration with all the other factors.
6.3

IDENTIFYING ALTERNATIVE STRATEGIES

Ideally the objective is to identify between three and five alternative strategies, each of which is in itself a complete answer to meeting the requirements: generally fewer than three gives little choice, whilst more than five overcomplicates the task and should not be necessary. If one strategy is a variation of another, consideration should be given as to whether to present it as a variation or as a separate strategy.

For all strategies to be considered, the Contingency Considerations report should be referred to, which should have identified more than one source for each contingency required.

The main contingencies the strategy will need to cover are:

- alternative premises;
- office computer equipment such as PCs, and backup data;
- specialist equipment, such as central computing facilities;
- furniture;
- office equipment such as photocopiers, binding machines;
- documents and stationery;
- communications services; and
- transport/delivery services.

Comprehensive information on considerations for these contingencies can be found in the CONT section of this Guide.
6.4 COMPILING A COST-EFFECTIVE RECOVERY STRATEGY

It is important to remember that the strategy only needs to cover a short period, from a few days to a couple of months, at as little cost as is consistent with the requirement to recover. For instance, if a property is unusable because of minor fire damage, there is no need to take a lease on new premises immediately, but only to rent temporary space until the original is repaired and operational again.

A cost-effective method may be to plan facilities for only a minimum number of staff to restart work. For example, in the case mentioned above, it would be cheaper to rent part of a smaller and older property for a small number of essential staff than to rent the whole of a large, modern office block to accommodate all staff.

6.4.1 Stages in Compiling a Strategy

The strategies which become apparent after reviewing and considering the available information should be evaluated, and any strategies which are not practical or obviously will not be acceptable should be rejected.

Suppliers and other sources for the resources and facilities needed should be identified and estimates of cost, time and effort needed to acquire the items should be obtained. These need not be exact, as reasonable approximate estimates are sufficient for strategy planning.

The possible strategies should be ranked by estimated cost, speed and certainty of recovery. The results are the basis of the strategy options to be presented in the Strategy Report.

Individual strategies should be developed until each gives a full solution to the recovery requirements and a clear picture of what it will achieve and cost.
6.5

THE PEOPLE FACTOR

The organisation of people during the recovery should be considered and included in the Recovery Strategy Report, to give management a fuller picture and to make it part of the overall strategy.

During the Recovery Phase, the normal organisational structure will be suspended and replaced by the Recovery Organisation which will concentrate on maintaining vital business operations. It must be made clear to management who are not in the Recovery Organisation that their attempts to help could interfere with the planned recovery. This policy should be made clear to everyone and agreed by management before the BCP is completed. It should be recognised that excellent line managers in normal circumstances may function less efficiently in the stress of emergency conditions.

An example of a Recovery Organisation is shown at REC 6.5.1.
6.5.1 Example of a Recovery Organisation Structure

The infrastructure teams provide the support which the Operation Recovery Teams and their staff will need to make their recovery and continue afterwards, for example:

- preparing the alternative premises for use, providing furniture, etc;
- setting up the computing services;
- supplying stationery;
- re-routing telephones; and
- helping staff with personal problems.
6.6

RECOVERY STRATEGY REPORT AND MANAGEMENT DECISION

The Recovery Strategy Report presents the options to management for approval and budgetary commitment to the recommended strategy. It should:

- refer to the BIR, in particular:
  - the Maximum Acceptable Outage Time (MAOT);
  - any other essential requirements to be met in recovery; and
  - the implications of any planned major changes;
- draw on the contingencies offered and any discussion of them in the Contingency Considerations report;
- state each strategy option and discuss its advantages and disadvantages. In doing so, it will make the point that cost is directly proportional to the speed and quality of recovery; and
- recommend the strategy which is considered to meet the recovery requirements and Departmental policy in the most cost-effective way.

Senior managers together should make the final choice of strategy because it will:

- affect all operations at the premises; and
- require senior managers’ endorsement of the budget needed to carry it out.
6.7 IMPLEMENTING THE STRATEGY

The chosen strategy will direct the rest of the BCP development project. Further development could be done entirely with in-house resources, or specialist consultants could either supervise the work or supplement resources.

6.7.1 Funding the Strategy

Consideration should be given to whether the initial costs and any ongoing costs for Business Continuity are outside the Department's normal authority or budget. This also applies to items which need to be acquired after the incident, according to the chosen strategy. If the costs are outside the budget, an alternative strategy may be needed, but the alternative should not be chosen if it does not sufficiently satisfy the requirements for recovery. Instead, it would be better to find a way to bring the costs within the budget. Alternatively, Departments may wish to take a view on approaching Treasury for additional funding where they consider that the costs of the strategy cannot be met from existing financial allocations.

6.7.2 Contingency Contracts

If the strategy calls for contracted contingencies, contract negotiation should start immediately. If the specific supplier(s) has not yet been identified, further work may be needed to identify and cost the best choice of supplier.

6.7.3 Computer Software

Commercial computer software packages are available to aid the remaining stages of the project, which vary in cost, quality and method. Packages which do not produce action-based Plans, do not allow easy maintenance or impose specific styles not totally acceptable to a Department should be avoided. PACE may be able to give advice on computer software.
WHAT SHOULD YOU DO?

1. From the BIR report identify:
   - the operations which must be restarted;
   - their minimum recovery levels; and
   - their minimum recovery times; and
   - the anticipated effects of forthcoming planned changes on
     the above.

2. Obtain confirmation of any Departmental policies which may
   affect choice of strategy.

3. Clarify the business units’ minimum recovery requirements.

4. From the Contingency Considerations report:
   - identify the contingencies which will support the required
     recoveries; and
   - group them into three to five sets of alternatives, based
     on:
     - increasing cost;
     - speed of recovery; and
     - certainty of recovery;

5. If necessary, carry out further research to determine the
   alternatives. Develop each alternative to give a practical and
   complete answer to the recovery requirements.

6. Evaluate each alternative for cost-effectiveness against speed and
   certainty of recovery.

7. From the operations to be recovered and their business units,
   design the Recovery Organisation.

8. Report with advantages and disadvantages of each strategy.

9. Seek management approval to the recommended strategy.

10. Make sure the costs for providing Business Continuity are within
    the Departmental authority or budget. If not, seek Treasury
    approval, if appropriate.

11. Take specialist advice as necessary.
### 7.0 PLAN DEVELOPMENT AND IMPLEMENTATION

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>ABOUT THIS SECTION</td>
</tr>
<tr>
<td>7.2</td>
<td>STRUCTURE AND CONTENT OF THE BCP DOCUMENT</td>
</tr>
<tr>
<td>7.3</td>
<td>WRITING THE BCP</td>
</tr>
<tr>
<td>7.4</td>
<td>RECOVERY TEAM COMPOSITION</td>
</tr>
<tr>
<td>7.5</td>
<td>RECOVERY TEAM TASKS</td>
</tr>
<tr>
<td>7.6</td>
<td>REVIEW OF FIRST DRAFT</td>
</tr>
<tr>
<td>7.7</td>
<td>IMPLEMENTATION AND TESTING</td>
</tr>
<tr>
<td>7.8</td>
<td>DISTRIBUTION</td>
</tr>
<tr>
<td>7.9</td>
<td>VERSION CONTROL</td>
</tr>
<tr>
<td>7.10</td>
<td>WHAT SHOULD YOU DO?</td>
</tr>
<tr>
<td>ANNEX 7/1</td>
<td>SPECIMEN PLANS</td>
</tr>
</tbody>
</table>
7.0 PLAN DEVELOPMENT AND IMPLEMENTATION

7.1 ABOUT THIS SECTION

This section:

• explains how to write a Business Continuity Plan (BCP) using:
  - the results of the previous development phases; and
  - further interviews with the business units whose essential operations are to be recovered; and

• provides:
  - details of what to include in a BCP;
  - advice on controlling distribution of the BCP; and
  - a set of specimen Plans at the end of the section.

Note: In shared premises, the landlord or major occupier (holder) is responsible for Incident Control for the entire premises on behalf of all occupants, but individual occupants are responsible for their own Business Continuity Planning.

7.1.1 Key Points

The key points to note for BCP development and implementation are:

• inputs to the BCP are:
  - the Business Impact and Recovery Strategy reports;
  - management decisions; and
  - further information from the business units;

• the BCP is built around the business units. It has a structure leading to and supporting the Task List of each business unit’s Recovery Team;

• the Task List is the action for recovery. It states what must be done, not how to do it;

• dependencies between operations must be supported during recovery;
• security in all its aspects must not be jeopardised;
• the BCP must be tested and teams trained;
• all changes to the BCP must be controlled; and
• old versions of the BCP must be destroyed.
7.2 STRUCTURE AND CONTENT OF THE BCP DOCUMENT

Before starting to write the BCP, its structure and content should be established. Consideration should be given to:

• the type of BCP needed, depending on how complex the organisation is; and
• the Recovery Teams and staff needed for the Recovery Organisation.

The BCP structure and the Recovery Organisation are based on the operations to be recovered and modified by the need to manage the recovery processes. If the structure of the BCP or the Recovery Organisation have not yet been agreed, they must be decided immediately, before starting to write the BCP.

7.2.1 Introduction

A typical BCP starts with an Introduction, which should include:

• explanatory background information to help readers to understand the BCP;
• the reasons for the BCP and its structure, to make sure these facts are clear to future management and Recovery Team members;
• the Department’s:
  - policy on Business Continuity; and
  - definition of a ‘disaster’;
• an outline of the chosen Recovery Strategy;
• the structure of the Recovery Organisation; and
• brief descriptions of the roles of the Recovery Teams, starting with the BCT.
7.2.2 Recovery Team Information

The next part of the BCP should be about the Recovery Team(s), starting with the BCT. If the chosen BCP structure incorporates all Recovery Teams in the one Plan, there will be a section for each Team which will state:

- the Team name;
- its recovery objectives;
- its responsibilities;
- all the members of that Team, with details of how they can be contacted;
- all the members of all the Recovery Teams in the section for the BCT;
- contact details for the BCT in the section for the Incident Control Team (ICT); and
- the Team Task List - the list of tasks it must perform to effect the recovery.

Team Task Lists are the most important component of a BCP. They are the basis of the recovery, giving specific direction to it. **Note:** The Task List states what must be done, not how to do it.

7.2.3 Supporting Information

The final part of the BCP is the Supporting Information which may be needed quickly during recovery. If the chosen BCP structure incorporates all Recovery Teams in one Plan, the supporting information for each Team should immediately follow each Team's Task List, so that their part of the BCP is on consecutive pages.

It is advisable that only essential supporting information is included in the BCP and not what is merely useful in order to minimise amendments caused by change and to prevent it from becoming unwieldy.
The supporting information could include details of:

- useful contacts within the organisation (other than members of the Recovery Teams);
- external suppliers for service or replacement of specialist equipment or specialist services, such as salvage or communications cabling;
- essential reference documents;
- special procedures for unusual tasks; and
- the minimum resource requirements for recovery of assets - items and quantity. If the minimum requirements are stated at this point in the BCP, the Team will see them whenever they refer to it. They will then be reminded to notify the Business Continuity Officer if the requirements change in case corresponding changes need to be made to any of the contingencies.

In addition to the above information, the supporting information for the BCT should include details of:

- the ICT and Incident Control Room; and
- details of any contract for:
  - contingency premises and how to access them; and
  - other contingencies, for example salvage or repairs.

Inventories of assets (beyond the statement of minimum resources required for recovery) are not needed for Business Continuity purposes. Information required for insurance and financial accounting purposes is normally held in an Assets Register by the Finance business unit.

Specimen Plans showing examples of the content of a BCP can be found at the end of this section.
7.3 **WRITING THE BCP**

7.3.1 **Sources of Information**

Writing of the BCP can begin once the following are established:

- the structure of the BCP;
- the structure of the Recovery Organisation;
- the required BCP content.

It is advisable to begin by reviewing the Business Impact Review and Recovery Strategy Reports and any management decisions concerning them briefly, as these provide the key input to the BCP.

It is recommended that the sections for individual business units’ Recovery Teams should be completed one at a time, to include its tasks and supporting information, before moving on to the next one. The Recovery Team Leader should be invited to contribute to the Plan writing as soon as possible.

A further interview with the manager of each business unit should be held to confirm the information to be included in the BCP. During the interview, the structure and content of the BCP and how it would operate should be explained, including:

- which operations are to be recovered;
- the Maximum Acceptable Outage Time (MAOT);
- the tasks required to achieve recovery of the operations; and
- the minimum staff and resources required.

7.3.2 **Co-ordination**

It is important to remember throughout the writing process that, whatever the BCP structure and however many Task Lists there are, every aspect of recovery must be cohesive and integrated so that each item recovered meets not only the specific needs of its operation but also the needs of any related operations. For example, if Payroll is due to run shortly after a disaster happens, then other supporting operations such as Accounts and Personnel which input to it must give this a priority in their recoveries which it would not do at other times. It is advisable during the interviews with business unit managers to check for dependencies not covered by the Business Impact Review.
7.4 RECOVERY TEAM COMPOSITION

7.4.1 Business Continuity Team (BCT)

The BCT normally consists of:

- senior managers; and
- business unit managers or their deputies.

7.4.2 Business Unit Recovery Teams

Each business unit manager should nominate the members of their business unit’s Recovery Team.

A business unit’s Recovery Team should consist of:

- three to six of the more senior or knowledgeable members of the business unit, but not necessarily the manager;
- a Leader;
- a Deputy to substitute in the Leader’s absence;
- enough members to cover all absences such as holidays, sickness, and other non availability.

All team members should be volunteers. If any Trades Union agreements present potential problems, for example concerning payment for being on call or called out or working unusual hours or conditions, these should be resolved before confirming team membership.

It is necessary to distinguish between a business unit’s Recovery Team and the remaining staff of the business unit. The Recovery Team members organise and manage the recovery of the business unit’s operations following a disaster, and the operations are then continued by themselves and other chosen staff.
For recovery purposes it may be helpful to consider the staff in three groups, say Red, Blue and Green:

- Red (including the Recovery Team) are needed as soon as recovery starts;

- Blue may be needed a few days or weeks later to enable the recovered operation to keep up with demand on its services (as identified in the Business Impact Review); and

- Green remain at home until told to return, which may not be until business returns to normal.
**RECOVERY TEAM TASKS**

The Recovery Team section of the BCP should include the procedures the Recovery Teams need to follow if a disaster happens, with specific Task Lists. The procedures should cover the following areas:

- emergency responses;
- security;
- damage assessment;
- contingencies;
- recovery of operations;
- contacting other staff, if appropriate;
- staff welfare; and
- salvage, if appropriate.

**7.5.1 The Role of the Business Continuity Team**

If a disaster occurs, the BCT is likely to be called out at an early stage to manage the recovery process. Their procedures should include specific tasks, such as:

- Incident Control: monitoring a potential incident to determine whether the ICT should be put on standby (the ICT may not have been called out if a physical incident has not yet occurred);
- damage assessment: assessing the effect of damage on working conditions to decide whether to invoke the BCP; and
- security: ensuring that security is maintained, particularly in alternative premises.

Procedures should also include checking that other Teams’ procedures are carried out, for example, liaising with the ICT to check that:

- evacuation has been completed;
- the emergency services have been called; and
- valuable objects have been removed, if appropriate.
If there is an Incident Control Room, it may prove beneficial for the BCT to work from it. The BCT should call out the individual Recovery Teams, who would follow their own procedures, then:

- monitor and manage the recovery at the higher level; and
- be prepared to resolve problems delaying recovery which the other Teams cannot manage alone.

**Contingencies**

Specific tasks for the BCT in this category could include:

- if PACE are to be asked for available alternative premises, specifying space requirements in the correct format;
- collecting the Recovery Box, if appropriate;
- collecting and holding petty cash; and
- arranging for salvage, if appropriate.

**Leased Premises**

For leased premises, the BCT should:

- examine the lease agreement to establish whether there is a requirement to continue paying rent whilst the property is unusable; and
- check with the Finance business unit that rent payments are continued if required, or stopped if not required. In the latter case it would be advisable to obtain the landlord’s agreement that the property is unusable.

**Media**

If appropriate, the BCT should contact Departmental Press Officers to inform them of the disaster and prepare them for dealing with any media enquiries. The Supporting Information for the BCT should therefore include contact details for Departmental Press Officers. Further information and advice can be found at News Media in section 10.6, Additional Considerations.
Damage Assessment

The **BCT** should work with the Premises Manager to assess damage to the premises. As each of these has a different objective, they will consider the damage in a different way:

- the **BCT** should be concerned with the effect of the damage on staff working conditions, and therefore needs only a superficial view; and

- the Premises Manager is concerned with the effect of the damage on the premises, and, therefore, will eventually need a very detailed assessment.

An example of a Damage Assessment Worksheet is given at sub-section **PLAN 7.5.2**. It could be included in the Supporting Information for the **BCT** and the Premises Manager to help them to:

- assess damage to the premises; and

- make a superficial record of the damage and the estimated time needed to repair it.

The Premises Manager should also consider the advice in **section IC 10.9.3 on Damage Assessment of the Assets.**
### Damage Assessment Worksheet

Keep to a brief summary, not a detailed report.

<table>
<thead>
<tr>
<th>Name/location of damaged room/area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of business unit using room</td>
</tr>
<tr>
<td>Type of damage</td>
</tr>
<tr>
<td>Extent of damage</td>
</tr>
<tr>
<td>Time to repair (rough estimate)</td>
</tr>
<tr>
<td>E.g. 1 hour or 1 day or 1 week etc</td>
</tr>
<tr>
<td>Comments</td>
</tr>
</tbody>
</table>
7.5.3 Emergency Responses

Depending on the nature of the disaster, one or more of the following responses may be required:

- bomb search, perhaps with evacuation from the premises or to a safer part of the premises;
- full evacuation, for example for a fire;
- calling the emergency services;
- removing valuable objects;
- calling out the ICT to an actual or potential disaster; and
- the ICT calling out the BCT to an actual or potential disaster.

Each of these could occur in isolation from the rest. The first five responses need immediate action, and all the responses are for different objectives, so all their procedures should be separate from each other. To be thorough, the procedures for some responses should include checking that others have been taken, if appropriate.

Procedures for bomb search and full evacuation must include calling the emergency services.

7.5.4 Security

Security must not be breached, weakened, reduced or removed just because a disaster has occurred. This means that all Plans and procedures should be designed to maintain security at its current level or at a level appropriate to the changed circumstances.

7.5.5 Contingencies

The chosen contingencies should be mentioned in the BCP as appropriate. In particular, if someone needs to obtain, collect or otherwise invoke the contingency, this should be included in the relevant teams’Task Lists, with a reference to the Supporting Information which should give details of what the contingency is, where it is, and how to get it.
The major contingencies Departments will need to consider are:

- alternative premises;
- furniture;
- office equipment such as photocopiers, binding machines;
- office computer equipment such as PCs;
- specialist equipment, such as central computing facilities;
- communications services; and
- transport/delivery services.

### 7.5.6 Recovery of Operations

Recovery of individual operations is left to the Recovery Teams, who should:

- ask the BCT to help resolve any problem delaying or threatening to delay recovery; and
- report progress at reasonable intervals or at specific times to:
  - the BCT; and
  - their business unit manager.

The Team Task Lists should cover these points.

### 7.5.7 Contacting Other Staff

If staff other than Recovery Team members need to be contacted, there are various ways to do so. The simplest and most commonly used is the cascade method: each business unit head is contacted first, they in turn contact managers, who in turn contact their own staff. This method is easy, quick and reliable, but it can only be done if each person making a contact has immediate access to contact details. Outside the usual premises this problem is usually solved either by managers keeping their own contact lists or by including contact lists in their copies of the BCP.
Staff Welfare

Incident Control will deal with cases of staff injury or death during the disaster; but some staff may suffer from delayed shock, either at home or while involved in the recovery. Consideration should be given to providing counselling for anyone affected, by external professional services if there is not a trained counsellor on the staff. Details of who will provide this service should appear in the Supporting Information for the BCT.

The Task List for each Recovery Team should include watching out for staff showing signs of shock. Advice on what these signs are should be included in the Task List.
7.6 REVIEW OF FIRST DRAFT

The first draft of each Team's procedures should be discussed in detail with its Team Leader and business unit manager, to identify errors and omissions and to obtain their agreement to it.

After updating, it will be ready for testing and copies should be issued formally to the business unit managers and Recovery Team members.
7.7 IMPLEMENTATION AND TESTING

When all parts of the BCP have been checked and agreed they need to be tested. Testing and training are fully covered at TEST later in this Guide.

Although the BCP is untested at this point, it offers the organisation a much higher likelihood of successful recovery than existed before, and therefore could be considered officially operational. The first tests, with their opportunities for training, should be held as soon as possible.
7.8 DISTRIBUTION

A balance must be drawn between distributing enough copies of the BCP to ensure that enough are available when needed under emergency conditions and being able to keep them up to date. If too many copies are distributed, there is a danger of using an out of date copy when the BCP is activated for a disaster. This could lead to confusion, error and delay in recovery. Team Leaders, their Deputies, members of each Team and others designated in the BCP should keep one copy of their part of the BCP at work and another at home. A full copy of the BCP should be stored in a safe place offsite, for example at the Incident Control Room or another nearby premises.
7.9

**VERSION CONTROL**

To maintain cohesion and integration, the Business Continuity Officer should control strictly any changes to Plans. Teams may suggest changes by submitting them in draft to the Business Continuity Officer for checking and discussion. However, the Business Continuity Officer should be the only person to issue revised versions which should bear the date and a version number on each page.

To reduce the risk of an old version being used, the Business Continuity Officer should devise a system for collecting all copies of old versions before issuing new ones. Staff should not make photocopies for themselves but instead obtain a copy from the Business Continuity Officer.
7.10 WHAT SHOULD YOU DO?

1. Establish the BCP structure and Recovery Organisation.

2. Review the reports of the Business Impact Review and Recovery Strategy for ideas on the content of the BCP.

3. Interview business unit managers to establish:
   - their minimum recovery requirements;
   - their Recovery Team’s:
     - members; and
     - procedures.

4. Consider all the points in section PLAN 7.3 above.

5. Produce the first draft of the BCP.

6. Discuss the draft of their part of the BCP with each business unit manager and Recovery Team Leader and agree amendments.

7. Make the amendments and issue the next draft.

8. Test each Plan as soon as possible.

9. Set up a system for:
   - controlling changes to the BCP; and
   - destroying old versions and issuing new ones.

10. Seek expert advice in areas where there is no in-house expertise.
ANNEX 7/1: SPECIMEN PLANS

The specimen Plans which follow are adapted from a three level structure which was produced for a regional office of a British national organisation. This sample was selected because it has the most complex structure and shows how the levels fit together. It does not contain all the ideas presented in the text because the original was written for a specific client’s requirements. Some of the terminology has been changed to make it more familiar to Civil Service users.

Information to be inserted as appropriate is shown in the specimen Plans in italics, inside square brackets.

Note: These specimens are presented only as examples and must not be treated as pro formas. BCP developers should not simply copy these specimens, but must produce original Plans, specific to their own premises.
[name of Department]

BUSINESS CONTINUITY PLANS FOR

[address of Department]

SITE MANAGEMENT LEVEL RECOVERY PLAN

DATE: [insert as appropriate]

VERSION: [insert as appropriate]

IN EMERGENCY START AT SECTION 2.2
DEPARTMENT MANAGEMENT RECOVERY PLAN

CONTENTS

1.0 INTRODUCTION

1.1 Policy
1.2 Definition of a Disaster
1.3 Strategy For Recovery
1.4 When the BCP will be Activated
1.5 How the BCP will be Activated

2.0 MANAGEMENT RECOVERY PLAN

2.1 Business Continuity Team Recovery Objectives and Responsibilities
2.2 Business Continuity Team Task List

3.0 SUPPORTING INFORMATION

3.1 Emergency Response Team Members
3.2 Incident Control Room
3.3 Welfare Adviser
3.4 Premises Manager
3.5 Recovery Centre
3.6 Area Recovery Team Leaders and Deputies
3.7 Other Internal Site Contacts
3.8 External Contacts - Departmental
3.9 External Contacts - non-Departmental
1.0 INTRODUCTION

1.1 POLICY

It is the policy of the Department to maintain a Business Continuity Plan (BCP) to ensure the prompt and efficient recovery of its essential business operations from any physical disaster occurring at its premises.

1.2 DEFINITION OF A DISASTER

A disaster is any event which prevents the Department from carrying on its usual operations at the normal place of work for more than [number] hours.

1.3 STRATEGY FOR RECOVERY

Essential operations will be recovered within [number] days by relocating staff and necessary resources to the Recovery Centre, near [place], where fully equipped office accommodation including PCs and terminals on line to the Department's systems will be available. Telephone services will be redirected from the Departmental premises to the Recovery Centre.

There are three levels of written recovery Plans:

1. Site Management (this Plan), which:
   - declares the disaster;
   - invokes the Plans;
   - monitors recovery at the highest level;

2. Area, which invokes the business unit Recovery Teams within its business area and manages their recovery process; and

3. Business unit, which recovers the essential business operations belonging to each business unit.
1.4 WHEN THE BCP WILL BE ACTIVATED

On notification of an apparently threatening incident, the Business Continuity Team (BCT) will examine the situation and decide whether or not a disaster exists. If the situation is not clear, they will obtain the necessary clarification. If the situation could escalate, a time limit for return to normal must be set and a disaster declared when the time limit expires or as soon as it becomes evident that the situation will not return to normal. Return must be reliable. The rest of the BCP will be activated as soon as a disaster is declared.

1.5 HOW THE BCP WILL BE ACTIVATED

When a disaster is declared, the following will be advised of the situation as soon as possible by the BCT:

- IT, who will provide IT services at the Recovery Centre;
- Premises Management, who will:
  - organise damage assessment;
  - organise repairs and restoration;
  - arrange for the return of backup data from offsite storage;
  - arrange for delivery of the emergency stationery supply to the Recovery Centre;
  - arrange for delivery of a set of procedures manuals to the Recovery Centre;
- Telecommunications Department, who will arrange for telephones to be redirected;
- Leaders of the Area Recovery Teams or their Deputies;
- the Chief Executive and/or other directors, as appropriate.

The Area Recovery Teams, using the cascade staff callout system, will contact the business unit Recovery Teams who will take part in the business recovery.

Invocation of the Recovery Centre will be made by one of [number] managers, all of whom are known to the Recovery Centre organisation.
If necessary, arrangements will be made to transport staff to the Recovery Centre. Arrival at the Recovery Centre will be set for [number] to [number] hours after invocation of the service and on arrival each Recovery Team will start its own recovery procedures.
2.0 MANAGEMENT RECOVERY PLAN

2.1 BUSINESS CONTINUITY TEAM RECOVERY OBJECTIVES AND RESPONSIBILITIES

2.1.1 Objectives

1. Declare that a disaster exists, if appropriate;
2. Facilitate the successful recovery of each essential business operation normally carried out at the premises;
3. Keep all staff in the business areas informed.

2.1.2 Responsibilities:

The BCT is responsible for the:

• complete and timely recovery of the essential operations; and
• safety and welfare of public and staff during the disaster and its aftermath.

2.2 BUSINESS CONTINUITY TEAM TASK LIST

2.2.1 Receive Notice of Disaster or Potential Disaster

This notice may come from any source at any time. Obtain as clear a picture as the informant can give.

2.2.2 Staff Safety

If the disaster has occurred within office hours, the first priority is the safety of the staff. Ensure that all are accounted for. As appropriate:

• the Emergency Evacuation Procedures must be carried out;
• First Aiders should attend casualties.

2.2.3 Emergency Services

Call Police, Fire and/or Ambulance Service as appropriate to the circumstances.
2.2.4 Open Incident Control Room

Decide whether the Incident Control Centre needs to be opened at [place]. If so advise [name] - see section 3.2, Incident Control Room.

2.2.5 Contact Welfare Adviser

If there are casualties, instruct the Welfare Adviser to attend. Otherwise give him/her notice that his/her services may be required - see section 3.3, Welfare Adviser.

2.2.6 Decide whether or not a Disaster situation Exists

If the event is one of the following and the impact will last longer than [number] hours, immediately declare that a disaster exists. (In this case Task 2.2.9, Decision Process below will be omitted):

- destruction of, or severe damage to, the premises making use impossible, for example fire, flood, collapse, contamination. If information is uncertain, unclear or insufficient, obtain immediate clarification;

- external event preventing access to the premises, for example police cordon, emergency evacuation, weather conditions;

- total loss of essential services, for example power, telephone, computing, heating;

- internal event largely preventing one or more of the following operations from continuing:
  - [names of the major operations at the premises]

2.2.7 Call other Team Members

Contact the other members of the BCT, advise them of the situation and arrange to meet - see section 2.3.1, Business Continuity Team Members.
2.2.8 First Meeting

If the Team Leader and Deputy are absent, choose a Team Leader to take overall responsibility and co-ordinate actions.

The decisions to be made are whether or not to:

- declare that a disaster exists;
- invoke the BCP in full;
- invoke only certain parts of the BCP;
- use the Recovery Centre.

2.2.9 Decision Process

If information is uncertain, unclear or insufficient, obtain immediate clarification.

If the event is a potential disaster, set the time limit for the MAOT and monitor progress. Recovery must be reliable. Do not extend the time limit because of promises of imminent restoration. An incident can be declared earlier if it becomes obvious that the time limit will be exceeded.

Assess the impact of the event on the ability to continue working in the premises. Note that an apparently minor event can cause much wider impact, such as smoke and water damage from a fire.

Decide whether the whole or only specific parts of the BCP should be implemented.

Make the decision: either declare a disaster and invoke the BCP, or stand down. Remember that the declaration can be cancelled.
2.2.10 **BCP Invocation**

Open a log of events, assigning one Team member to maintain it. Use it to record:

- lost property, both personal and Departmental;
- expenses;
- problems encountered;
- events - the main points only, not a detailed account.

Inform the following - see section 3.0, Supporting Information following this Task List for contact details:

- the Chief Executive, Director etc;
- Leaders or Deputy Leaders of the Recovery Teams, see Task 2.2.13, Area Recovery Teams below;
- Royal Mail;
- switchboard;
- [others as appropriate].

Tell them as appropriate:

- the type, impact and time of incident;
- whether there are any casualties;
- where you can be reached;
- what support you need from them;
- whether the Recovery Centre is required;
- agreed frequency of further updates.

2.2.11 **Use the Recovery Centre**

If the decision has been made to utilise the Recovery Centre the nominated staff should carry out the invocation procedure. See section 3.5, Recovery Centre. If the decision has not yet been made but seems very likely, the Centre may be put on notice. It must then be advised within an hour or two as to whether or not relocation is going ahead.
2.2.12 **Notify the Minister (if appropriate)**

Provide the Minister’s Private Secretary with briefing on the situation.

2.2.13 **Area Recovery Teams**

Contact the Team Leaders or Deputies of the Area Recovery Teams - see section 3.6, *Area Recovery Team Leaders and Deputies* - and brief them on the situation. Advise whether they are to invoke their individual parts of the BCP and confirm whether they will be relocated.

If relocating, instruct the Team Leaders to submit their lists of all staff who are to go to the Recovery Centre.

Remind relocating Team Leaders that they are to act as ‘travel couriers’ to ensure that all their staff reach the Recovery Centre.

2.2.14 **News Media Communication**

Remind everyone that they must not speak to the press, radio or television but that all enquiries should be referred to the Press Office at [place], see section 3.8, *External Contacts - Departmental*.

2.2.15 **Change of Recovery Centre**

If the designated Recovery Centre is not available, an alternative Recovery Centre will be allocated by the supplier and you will be advised not more than an hour after the relocation decision is made. Note the details of the alternative and have that information distributed to everyone.

2.2.16 **Relocation Logistics**

Assign a Team Member to be the Logistics Officer and do the following. Remind him/her that time is important:

- if use of the [place] Recovery Centre is anticipated, immediately make enquiries about travel methods. The preferred method is a coach from the premises affected by the incident;

- make arrangements for the collection of all recovery material stored offsite and for its transportation to the Recovery Centre for the relocating staff; or
• if the [place] Recovery Centre is not available and another is assigned, make immediate enquiries about travel methods, departure times, and accommodation, if appropriate. Seek advice from travel agents - see section 3.9, External Contacts - non-Departmental - and have the agent supply someone to assist at the departure;

• as soon as possible, advise all relocating staff of the arrangements:
  - when and where to meet;
  - how long they will be away;
  - what they should bring with them, if anything;

• if staff are to stay at a hotel, arrange for twice daily transport between the hotel and the Recovery Centre.

Be prepared to:

• distribute any travel documents at the departure meeting point;

• ensure that the recovery material is sent to the Recovery Centre; and

• generally supervise departure.

2.2.17 Staff Communications

Notify all staff and contractors as quickly as possible, using the cascade process as appropriate. This should include relevant information regarding temporary arrangements, especially if staff are to relocate to the Recovery Centre.

Remember to advise the switchboard operators, messengers, and security guards - see section 3.7, Other Internal Site Contacts.

2.2.18 Internal Communication

Draft a message advising the rest of the Department of the situation and issue it to Internal Communications for distribution - see section 3.8, External Contacts - Departmental.
2.2.19 **Liaise with Salvage Service**

If a salvage service has been called out, assign one Team Member to be the liaison contact with the salvagers. Normally this will be the Premises Manager.

2.2.20 **Check Logistics**

Check with the Logistics Officer that the making of travel arrangements, movement of files etc is proceeding satisfactorily.

2.2.21 **Relocation Lists**

Follow up any lists of staff to be relocated which Team Leaders have not yet submitted. Copy these to the Logistics Officer. Prepare and fax to the Recovery Centre a full list of all people who are to arrive there, together with the headcount. This is to facilitate:

- entry on arrival;
- distribution of security passes.

The fax should be sent well in advance of arrival. It will be helpful for the Recovery Centre to know the headcount at the very earliest opportunity.

2.2.22 **Advise Office Services**

Contact the office cleaners and any other services which call on a regular basis and cancel their visits until further notice. See section 3.9, External Contacts - non-Departmental. Try to establish whether any deliveries to the premises are expected, for example stationery, and divert to the new premises if practical.

2.2.23 **At the Recovery Centre**

On arrival at the Recovery Centre, check that each Recovery Team:

- has arrived safely;
- has moved into its allocated space;
- has its recovery material;
- is able to access its systems on the terminals provided;
- has started its recovery.
Check that:

- telephones have been redirected from the premises to the Recovery Centre;
- any problems are being addressed.

2.2.24 **Update the Minister (if appropriate)**

Provide the Minister’s Private Secretary with an update on the current situation with confirmation that recovery is under way.

2.2.25 **Monitor Recovery**

At intervals, check that recovery is proceeding as expected. If unforeseen problems are delaying recovery, take action to have them resolved without delay.

2.2.26 **Staff Welfare**

Assign a Management Team member to:

- check whether the staff are encountering any problems;
- give assistance in order to resolve them.

Alternatively, use the services of the Welfare Adviser - see section 3.3, Welfare Adviser.

2.2.27 **Liaise with Premises Manager**

Liaise with the Premises Manager over the restoration or replacement of the premises.
2.2.28 **Return to Normal Operations**

When the Premises Manager advises that the premises are ready for reoccupation, arrangements for the return need to be planned.

Staff need to be instructed to:

- save all data for transfer to original premises;
- delete Departmental data from the Recovery Centre's PCs and file servers; and
- remove Departmental and personal property from the Recovery Centre.

Arrange for:

- the Team logs to be collected; and
- expenses and insurance loss details to be passed to the Finance business unit.

2.2.29 **Review of Events**

With the Team Leaders and Management and using the Team logs for input:

- hold a review of:
  - the disaster;
  - the recovery;
  - the performance of the BCP;
- identify any measures for prevention of future occurrences and improvements to the BCP, and have them actioned.
3.0 SUPPORTING INFORMATION

3.1 EMERGENCY RESPONSE TEAM MEMBERS

Name | Home telephone | Mobile telephone/Pager

3.2 INCIDENT CONTROL ROOM

Location | Telephones: | Fax:

3.3 WELFARE ADVISER

On request, the Incident Control Team (contact via BCT) will obtain a professional Welfare Adviser (from an outside agency if there is not already a trained counsellor on the staff).

The Welfare Adviser will provide counselling for casualties, both physical and psychological.

3.4 PREMISES MANAGER

Name | Home telephone | Mobile telephone/Pager

Outside office hours contact the Security Desk, which holds home and other contact numbers for all senior management personnel.

3.5 RECOVERY CENTRE

The following are authorised to invoke the Recovery Centre contract with [supplier name]. Each holds a copy of the invocation procedure.

[names]

Recovery Centre Fax number
(for sending headcount and list of relocating staff)

See the following pages for:

• a map of the Recovery Centre location;
• public transport information.
[page with map to show the location of the Recovery Centre]
[page to show details of transport to the Recovery Centre]
3.6 **AREA RECOVERY TEAM LEADERS AND DEPUTIES**

<table>
<thead>
<tr>
<th>Team</th>
<th>Name</th>
<th>Home telephone</th>
<th>Mobile telephone/Pager</th>
</tr>
</thead>
</table>

[Four detail lines per team of Leader and Deputy plus two other Recovery Team members]

3.7 **OTHER INTERNAL SITE CONTACTS**

Messengers:

Switchboard:

Security guards and their agency:

[+ others as appropriate]

3.8 **EXTERNAL CONTACTS - DEPARTMENTAL**

**Minister’s Private Secretary**

<table>
<thead>
<tr>
<th>Name</th>
<th>Office hours telephone</th>
<th>Out of office hours telephone</th>
<th>Mobile telephone/Pager</th>
</tr>
</thead>
</table>

**Press Office**

<table>
<thead>
<tr>
<th>Name</th>
<th>Telephone</th>
<th>Fax</th>
</tr>
</thead>
</table>

**Internal Communications:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Telephone</th>
<th>Fax</th>
</tr>
</thead>
</table>

3.9 **EXTERNAL CONTACTS - NON-DEPARTMENTAL**

**Emergency Services**

Fire Brigade:

Police Station:

Hospital:
### Utilities

Electricity:

Gas:

Royal Mail helpline:

[+ others as appropriate]

### Couriers

<table>
<thead>
<tr>
<th>Name</th>
<th>Telephone</th>
</tr>
</thead>
</table>
| FM/Works Consultants

<table>
<thead>
<tr>
<th>Name</th>
<th>Telephone</th>
</tr>
</thead>
</table>

### Salvage Services

<table>
<thead>
<tr>
<th>Name</th>
<th>Telephone</th>
</tr>
</thead>
</table>
[name of Department]

BUSINESS CONTINUITY PLANS FOR

[address of Department]

AREA LEVEL RECOVERY PLAN

FOR CENTRAL SERVICES DIVISION

DATE: [insert as appropriate]

VERSION: [insert as appropriate]

IN EMERGENCY START AT SECTION 5.2
## CENTRAL SERVICES DIVISION RECOVERY PLAN

### CONTENTS

#### 4.0 INTRODUCTION

- 4.1 Policy
- 4.2 Definition of a Disaster
- 4.3 Strategy for Recovery
- 4.4 When the Business Continuity Plan will be Activated
- 4.5 How the Business Continuity Plan will be Activated

#### 5.0 CENTRAL SERVICES DIVISION RECOVERY PLAN

- 5.1 Central Services Division Operations to be Recovered
- 5.2 Team Recovery Objectives and Responsibilities - Essential Operations
- 5.3 Recovery Team Task List

#### 6.0 SUPPORTING INFORMATION

- 6.1 Central Services Division Recovery Team Members
- 6.2 Incident Control Room
- 6.3 Business Unit Recovery Team Leaders and Deputies
- 6.4 Staff Numbers for Relocation
- 6.5 External Contacts - Departmental
- 6.6 External Contacts - non-Departmental
4.0 INTRODUCTION

4.1 POLICY

It is the policy of the Department to maintain a BCP to ensure the prompt and efficient recovery of its essential business operations from any physical disaster occurring at its premises.

4.2 DEFINITION OF A DISASTER

A disaster is any event which prevents the Department from carrying on its normal operations at the normal place of work for more than [number] hours.

4.3 STRATEGY FOR RECOVERY

Essential operations will be recovered within [number] days by relocating staff and necessary resources to the Recovery Centre, near [place], where fully equipped office accommodation including PCs and terminals on line to the Department’s systems will be available. Telephone services will be redirected from the Departmental premises to the Recovery Centre.

There are three levels of written recovery Plans:

1. Site Management, which:
   - declares the disaster;
   - invokes the Plans;
   - monitors recovery at the highest level;

2. Area (of which this is one), which invokes the business unit Recovery Teams within its business area and manages their recovery process; and

3. Business Unit, which recovers the essential business operations belonging to each business unit.
4.4 **WHEN THE BUSINESS CONTINUITY PLAN WILL BE ACTIVATED**

On notification of an apparently threatening incident, the Business Continuity Team (BCT) will examine the situation and decide whether or not a disaster exists. If the situation is not clear they will obtain the necessary clarification. If the situation could escalate, a time limit for return to normal must be set and a disaster declared when the time limit expires or as soon as it becomes evident that the situation will not return to normal. Return must be reliable. The rest of the BCP will be activated immediately that a disaster is declared.

4.5 **HOW THE BUSINESS CONTINUITY PLAN WILL BE ACTIVATED**

When a disaster is declared, the following will be advised of the situation as soon as possible by the BCT:

- IT, who will provide IT services at the Recovery Centre;
- Premises Management, who will:
  - organise damage assessment;
  - organise repairs and restoration;
  - arrange for the return of backup data from offsite storage;
  - arrange for delivery of the emergency stationery supply to the Recovery Centre;
  - arrange for delivery of a set of procedures manuals to the Recovery Centre;
- Telecommunications Department, who will arrange for telephones to be redirected;
- Leaders of the Area Recovery Teams or their Deputies.

The Area Recovery Teams, using the cascade staff callout system, will contact the business unit Recovery Teams who will take part in the business recovery.

Invocation of the Recovery Centre will be made by one of [number] managers, all of whom are known to the Recovery Centre organisation.
If necessary, arrangements will be made to transport staff to the Recovery Centre. Arrival at the Recovery Centre will be set for [number] to [number] hours after invocation of the service and on arrival each Recovery Team will start its own recovery procedures.
5.0 CENTRAL SERVICES DIVISION RECOVERY PLAN

5.1 CENTRAL SERVICES DIVISION OPERATIONS TO BE RECOVERED

5.1.1 To Recover within One Day

Reprographics Team [operations by name]

File Registry Team [operations by name]

[+ others as appropriate]

5.1.2 To Recover within Three Days

Reprographics Team [operations by name]

File Registry Team [operations by name]

[+ others as appropriate]

5.1.3 To Recover within Ten Days

[Team] [operations by name]

5.1.4 To Recover after Three Days

[Team] [operations by name]
5.2 TEAM RECOVERY OBJECTIVES AND RESPONSIBILITIES - ESSENTIAL OPERATIONS

5.2.1 Objectives

1. To activate the Recovery Plans of the business units within the Division;

2. To ensure the successful recovery of each essential business operation normally carried out by the Division;

3. To keep all staff in the Division informed.

5.2.2 Responsibilities

The Central Services Division Recovery Team is responsible for the:

- complete and timely recovery of its essential operations; and

- safety and welfare of its staff during the disaster and its aftermath.

The essential operations to be recovered are listed under their Recovery Teams in section 6.0.

5.3 RECOVERY TEAM TASK LIST

5.3.1 Receive Notification of a Disaster

The BCT will advise:

- that the BCP has been invoked;

- whether the Recovery Centre will be used, and if so, the number of staff to relocate;

- whether the Incident Control Room will be used;

- the nature of the event;

- any specific instructions. (All information concerning the Recovery Centre will be provided by the BCT at the appropriate time.)
5.3.2 **Call Other Team Members**

Contact the other members of the Central Services Division Recovery Team, advise them of the situation and arrange to meet - see section 5.3.1, *Central Services Division Recovery Team Members.*

5.3.3 **Brief the Team**

Assemble the Team and:

- brief them on:
  - the nature of the event;
  - any special instructions;
- identify any special considerations for recovery which may apply at the time;
- ensure there is a common understanding of priorities and planned actions;
- discuss the problems which may arise when the Division’s Recovery Teams move, if staff are to relocate to the Recovery Centre, for example:
  - deciding who should go and who should not go. This will depend on the level of staff to be relocated - see section 6.4, *Staff Numbers for Relocation;*
  - when and where staff should meet;
  - how the Recovery Teams will marshal their staff;
- remind members of the business unit Recovery Teams of the standing instructions not to talk to the news media.

5.3.4 **Logs**

Assign a Team member to open a log in which to record:

- losses, Divisional and personal;
- expenditure of petty cash and other expenses;
- any unexpected problems; and
- events, main points only.
5.3.5 Advise Business Unit Recovery Teams

Contact the Leaders of the business unit Recovery Teams or their Deputies - see section 6.3, Business Unit Recovery Team Leaders and Deputies - and advise them:

- to invoke their part of the BCP;
- whether the Recovery Centre will be used;
- of the nature of the event;
- how and when the Central Services Division Recovery Team is to be contacted;
- to submit to the Central Services Division Recovery Team, as soon as possible, a list of their staff who are to relocate, together with the headcount;
- to notify their staff as quickly as possible;
- of any specific instructions;
- to remind staff of the standing instructions not to talk to the news media.

5.3.6 Advise Head of Central Services Division

Contact the Head of the Central Services Division and brief him/her on the situation.

5.3.7 Other Communications

Contact anyone else who should be advised by Divisional level.

5.3.8 Divisional Stationery

Instruct the stationery supplier to send immediately to the Recovery Centre one fifth of the monthly consumption of the special Divisional stationery.
5.3.9 **Follow up**

After a suitable interval, check that each business unit Recovery Team has:

- held their Team Briefing;
- advised all their staff;
- submitted their lists of staff to be relocated;
- determined lost data/working papers or how to work round losses.

5.3.10 **Staff Lists**

Collate the lists from the business unit Recovery Teams. Check the headcounts. Submit a single list with confirming headcount for the Division to the BCT. This needs to be done in good time to facilitate entry to the Recovery Centre.

5.3.11 **Salvage**

Ask the Premises Manager if it is possible to salvage papers and files. If so, consult with the business unit Recovery Teams as to what needs to be salvaged and their locations. (It may be necessary to do this through the salvage service.)

If not, consult with the business unit Recovery Team Leaders on how they intend to operate in view of the losses, and agree the best method.

5.3.12 **At the Recovery Centre**

On arrival at the Recovery Centre, check that each Recovery team:

- has arrived safely;
- has moved into its allocated space;
- has received its recovery material;
- has started its recovery;
- is able to access its systems on the PCs provided; and
- has had its telephones redirected.
Ensure that any problems which are delaying or may delay recovery are being addressed and try to get them resolved at the earliest opportunity.

5.3.13 **Staff Welfare**

Check that staff encountering personal problems are given assistance in solving them. Look out for signs of shock or stress. Be aware of the need to arrange for counselling, by outside experts through the BCT if there are no suitable in-house staff.

5.3.14 **Update Head of Central Services Division**

Contact the Head of Central Services Division to brief him/her of the current situation and to confirm that recovery has started.

5.3.15 **Lost Data/Working Papers**

Each business unit Recovery Team should have established the status of existing work in progress to identify lost work. Check that they have determined:

- if it is possible to recover any lost work; or
- how to work round any losses.

5.3.16 **Monitor Recovery**

At suitable intervals, check that recovery is proceeding as expected. If unforeseen problems are delaying recovery, take action to have them resolved without delay.

5.3.17 **Update Emergency Response Team**

At intervals as required by the BCT, report the status of the Recovery Teams in this area and any other significant information.
5.3.18 **Report Logged Information**

At intervals as required by the BCT and at the end of the disaster period, collect and collate the logged information from the Division’s Teams, separating it into losses, expenses, problems and events, and pass it to the BCT.

5.3.19 **Liaise with Premises Manager**

If required, liaise with the Premises Manager about the Division’s requirements for space, furnishings, office equipment, etc in the repaired or replacement premises.

5.3.20 **Return to Normal Operations**

Arrangements need to be planned for the move to the original premises (or their replacement) once ready for occupation.

Staff need to be instructed to:

- save all data for transfer to premises;
- delete Departmental data from Recovery Centre PCs and file servers;
- remove Departmental and personal property; and
- hand in Recovery Centre security passes.

Arrange for the:

- Recovery Team logs to be collected; and
- expenses and insurance loss details to be passed to the Finance business unit.

5.3.21 **Review of the Incident**

Be prepared to attend a review of the disaster, the recovery, and the performance of the BCP. The Recovery Team logs will provide input to the review, whose purpose is to identify any measures for prevention of future occurrences and improvements to the BCPs. When agreed, these will need to be actioned.
6.0 SUPPORTING INFORMATION

6.1 CENTRAL SERVICES DIVISION RECOVERY TEAM MEMBERS

Name        Home telephone        Mobile telephone

Substitutes:

6.2 INCIDENT CONTROL ROOM

Location    Telephones

6.3 BUSINESS UNIT RECOVERY TEAM LEADERS AND DEPUTIES

Team        Name        Home telephone  Mobile telephone/ telephone  Pager

Leader:

Deputy:

Leader:

Deputy:

6.4 STAFF NUMBERS FOR RELOCATION

The Recovery Centre has spaces for 200 staff only whereas the [name] Department headcount exceeds 1,000. The number of staff to be relocated from any one business unit or area depends on how much of the existing premises is still usable. The following table states how many Central Services Division staff may need to be relocated and in which circumstances.

<table>
<thead>
<tr>
<th>Unusable Premises</th>
<th>Relocateable Staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>64</td>
</tr>
<tr>
<td>A floor only</td>
<td>110</td>
</tr>
<tr>
<td>B floor only</td>
<td>84</td>
</tr>
<tr>
<td>C floor only</td>
<td>54</td>
</tr>
</tbody>
</table>
6.5 **EXTERNAL CONTACTS - DEPARTMENTAL**

[restrict to those which the Division would contact, not Site Management or business unit]

6.6 **EXTERNAL CONTACTS - NON-DEPARTMENTAL**

[restrict to those which the Division would contact, not Site Management or business unit]
[name of Department]

BUSINESS CONTINUITY PLANS FOR

[address of Department]

BUSINESS UNIT RECOVERY PLAN

FOR REPROGRAPHICS

DATE: [insert as appropriate]

VERSION: [insert as appropriate]

IN EMERGENCY START AT SECTION 8.0
CONTENTS

7.0 REPROGRAPHICS RECOVERY TEAM

7.1 Team Recovery Objectives
7.2 Team Recovery Responsibilities
7.3 Essential Operations to be Recovered
7.4 Recovery Team Members and their Contact Details

8.0 REPROGRAPHICS RECOVERY TEAM TASK LIST

8.1 Receive Notification of a Disaster
8.2 Call Out Team
8.3 Brief Team
8.4 Logs
8.5 Advise Reprographics Staff
8.6 Salvage
8.7 Moving to the Recovery Centre
8.8 At the Recovery Centre
8.9 Commence Recovery
8.10 Determine Lost Data/Working Papers
8.11 Working Reference Material
8.12 Other specific recovery tasks which are necessary for the business unit to restart work
8.13 Check Recovery Progress
8.14 Reporting
8.15 Report Logged Information
8.16 Return to Normal Operations
9.0 SUPPORTING INFORMATION

9.1 Staff Numbers for Relocation
9.2 Business Contacts
9.3 Essential Documents
9.4 Requirements for Recovery
7.0  **REPROGRAPHICS RECOVERY TEAM**

7.1  **TEAM RECOVERY OBJECTIVES**

1. To re-establish the essential Reprographics operations within the timescales in section 7.3 below;

2. To provide a level of service such that users of Reprographics services would otherwise be unaware of the disaster.

7.2  **TEAM RECOVERY RESPONSIBILITIES**

To ensure that the desired level of Reprographics service is maintained throughout the period of the disaster.

7.3  **ESSENTIAL OPERATIONS TO BE RECOVERED**

Within one day: [operations by name]

Within three days: [operations by name]

Within ten days: [operations by name]

After ten days: [operations by name]

7.4  **RECOVERY TEAM MEMBERS AND THEIR CONTACT DETAILS**

Name  | Home telephone  | Mobile telephone/ Pager
--- | --- | ---
Leader:
Deputies:
Substitutes:
8.0 REPROGRAPHICS RECOVERY TEAM TASK LIST

8.1 RECEIVE NOTIFICATION OF A DISASTER

The Central Services Division Recovery Team will advise:

- that the BCP has been invoked;
- the number of staff who are to relocate;
- the nature of the event;
- any specific instructions.

(All information concerning the Recovery Centre will be provided through the Divisional Team at the appropriate time.)

8.2 CALL OUT TEAM

Contact the other members of the Reprographics Recovery Team - see section 7.4, Recovery Team Members and their Contact Details - and instruct them where and when to meet. If necessary call substitutes to make up numbers.

8.3 BRIEF TEAM

Assemble the Recovery Team and:

- brief them on:
  - the nature of the event; and
  - any special instructions;
- identify any special considerations for recovery which may apply at the time;
- ensure there is a common understanding of priorities and planned actions.
If staff are to relocate to the Recovery Centre, discuss the logistics of moving the business unit, for example:

- who should go/should not go. This will depend on the level of staff is to be relocated - see section 9.1, Staff Numbers for Relocation;
- when and where staff should meet;
- how the Recovery Team will marshal the staff;
- what problems could arise and how they could be solved.

As soon as possible:

- prepare a list of all your Recovery Team and staff who are to relocate;
- do a head count of the number of staff to relocate and add this total to the list;
- submit the list to the Divisional Recovery Team;
- prompt the Recovery Team to remind other staff of the standing instructions not to talk to the news media but to refer them to the Press Office at [place].

8.4 LOGS

Assign a Team member to open a log in which to record:

- losses (business unit’s and personal);
- expenditure of petty cash and other expenses;
- any unexpected problems.

8.5 ADVISE REPROGRAPHICS STAFF

If this is not the first communication to your staff, find out what advice may already have been given to staff about the event and about moving to the Recovery Centre.

Consider what further information you should give them and arrange for this to be done using the cascade method.
8.6 SALVAGE

Consider what papers, files or other material can and should be rescued in the circumstances or retrieved from backup. If a salvage service has been called in, consult them about salvage, otherwise organise Recovery Team members to do this.

8.7 MOVING TO THE RECOVERY CENTRE

Assemble the staff at the meeting point and, if there are absentees, try to contact them. Marshal your staff and ensure that they all arrive at the destination. If staff are to stay at a hotel, check that everyone is booked into the hotel and finds their rooms.

Try to deal with problems yourself, if possible, rather than escalate them to the Divisional Recovery Team.

8.8 AT THE RECOVERY CENTRE

On arrival at the Recovery Centre you and your staff will be issued with:

- personal site passes by Recovery Centre staff; and
- user LogOn IDs by Departmental IT staff.

Both processes will take about five minutes per person. Ensure that all your staff go through these processes.

Deal with other settling-in matters, such as using the passes to access permitted parts of the premises, finding the allocated seating positions, familiarisation with premises.

8.9 COMMENCE RECOVERY

Instruct your staff to recover their essential business operations.

Check that the IT systems needed are available to each of your staff at their work positions. Refer problems to Departmental IT.

Check that all telephone equipment is working and that calls are being redirected successfully. Refer problems to Recovery Centre management.
8.10 **DETERMINE LOST DATA/WORKING PAPERS**

Check the computer files for the last input and examine papers salvaged from the office to try to identify what data or working papers have been lost, if any. Consider whether anything can be done to recover the lost data and papers. If not, consider how best to work round the losses.

Liaise with the other Team Leaders to exchange ideas and to ensure that reprinting does not cause a log jam.

8.11 **WORKING REFERENCE MATERIAL**

Consider whether the following would help to resume work in hand:

- [list of computer printouts, manuals etc as appropriate]

8.12 **OTHER SPECIFIC RECOVERY TASKS WHICH ARE NECESSARY FOR THE BUSINESS UNIT TO RESTART WORK**

- [list of tasks as appropriate]

8.13 **CHECK RECOVERY PROGRESS**

As soon as it is practical to do so, check that:

- all your essential operations are being carried out;
- any problems are being addressed.

8.14 **REPORTING**

At intervals, as required by the Divisional Recovery Team, report your Recovery Team's status and other significant information to the Divisional Recovery Team.

Advise them **immediately** of any problems which are delaying recovery.

8.15 **REPORT LOGGED INFORMATION**

At intervals, as required by the Divisional Recovery Team and at the end of the disaster period, separate the logged information into losses, expenses and problems, and pass it to the Divisional Team.
8.16 **RETURN TO NORMAL OPERATIONS**

When advised to prepare for return to the normal work premises, ensure that your staff:

- save all data files;
- delete Departmental data from the Recovery Centre’s PCs and file servers;
- remove Departmental property and their personal property when they leave; and
- hand in their Recovery Centre passes.
9.0 SUPPORTING INFORMATION

9.1 STAFF NUMBERS FOR RELOCATION

The Recovery Centre has spaces for 200 staff only whereas the Department’s headcount exceeds 1,000. The number of staff to be relocated from any Department depends on whether any of the premises is still usable. The table following states how many Reprographics staff may be relocated in which circumstances.

<table>
<thead>
<tr>
<th>Unusable Premises</th>
<th>Relocatable Staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>10</td>
</tr>
<tr>
<td>A floor only</td>
<td>25</td>
</tr>
<tr>
<td>A and B floors</td>
<td>35</td>
</tr>
<tr>
<td>A and C floors</td>
<td>35</td>
</tr>
</tbody>
</table>

9.2 BUSINESS CONTACTS

[list those which are likely to be needed but do not appear in the Department’s internal directory, and which would take time to look up]

9.3 ESSENTIAL DOCUMENTS

[list those which are fairly certain to be needed]

9.4 REQUIREMENTS FOR RECOVERY

The following are the minimum recovery requirements:

- 35 desk positions each with mainframe connected PC and telephone.
- file storage:
  - 10 filing cabinets;
  - one safe;
• special equipment:
  - 15 calculators;
  - one microfiche viewer;

• special stationery - see separately maintained list of items and quantities;

• special computing applications:
  - PC: DW4, Customer Experience Measures, Spread Sheet (Lotus);
  - Mainframe: Customer File;

• skills inventory - staff in other Departments with the necessary skills:

<table>
<thead>
<tr>
<th>Skill</th>
<th>Name</th>
<th>Last known location</th>
</tr>
</thead>
</table>

# BCP AWARENESS, TESTING, TRAINING AND MAINTENANCE

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1</td>
<td>About This Section</td>
</tr>
<tr>
<td>8.2</td>
<td>Creating Awareness</td>
</tr>
<tr>
<td>8.3</td>
<td>Testing</td>
</tr>
<tr>
<td>8.4</td>
<td>Training the Recovery Teams</td>
</tr>
<tr>
<td>8.5</td>
<td>Exercise Methods</td>
</tr>
<tr>
<td>8.6</td>
<td>BCP Maintenance</td>
</tr>
<tr>
<td>8.7</td>
<td>What Should You Do?</td>
</tr>
<tr>
<td>Annex 8/I</td>
<td>Sample Scenario</td>
</tr>
</tbody>
</table>
8.0 BCP AWARENESS, TESTING, TRAINING AND MAINTENANCE

8.1 ABOUT THIS SECTION

This section explains:

- why awareness of the Business Continuity Plan (BCP) project is important, and how to create it;
- the need for testing and training, and methods to accomplish both;
- the effects of change on the BCP, and the need to maintain the BCP's effectiveness through monitoring and periodic review.

8.1.1 Key Points

The key points to note for BCP awareness, testing, training and maintenance are:

- the success of the BCP is in everyone's interest;
- the level of staff awareness of the BCP can be raised by a campaign of regular information about the BCP development;
- every test of the BCP gives training experience, and vice versa;
- testing must be planned;
- testing (and training) must not be allowed to be the cause of a disaster;
- changes indicated by testing should be incorporated into the BCP which should then be re-tested;
- tests should start small and progress to full tests;
- all Recovery Team members should gain practical experience through testing and training within six months of implementation of the BCP;
- a regular programme of refresher training, at least annually, should be set up;
• major changes in the premises or Department(s) which affect the BCP may require additional training;

• **BCP** maintenance should be done at specified intervals, at least annually, or following a major change if sooner;

• holders of the **BCP** must have the latest version, and all old versions must be destroyed.
8.2  

**CREATING AWARENESS**

Staff awareness of the BCP and its purpose will improve the BCP and its operation by creating enthusiasm and co-operation. For their own safety, having a good BCP in place is important to all staff.

From the start of the BCP development project, positive action to create awareness of the BCP during the development, testing and training phases should be taken by:

- the BCP Owner;
- the Business Continuity Officer;
- the Recovery Team Leaders; and/or the Owners of the individual business unit recovery Plans.

Creating awareness of the BCP development project could be done by:

- holding briefings for all staff at an early stage of BCP development to explain:
  - the reasons for the BCP and its benefits to everyone;
  - how it will be developed;
  - how staff are involved in it;
- keeping the BCP at a high profile, with the help of the managers of the business units, by informing staff of progress made at regular intervals;
- ensuring that:
  - all the key players receive practical experience through testing the BCP within, at the most, six months of completing the BCP;
  - all the Recovery Teams practise their recovery regularly, at least annually;
  - all new staff are briefed about the BCP as part of their induction to the Department.
8.3 TESTING

Before any testing starts, it must have:

• a strategy; and
• a Plan.

8.3.1 Test Strategy

The recommended testing strategy is to:

• start by testing components of the BCP separately;
• combine tested components into wider tests; and
• build up to a test of the whole BCP.

A suitable component could be the recovery of one particular operation or one aspect of it in isolation. Components should be identified on the basis of what it is practical to test at one time.

The strategy for planning and each test Plan should be recorded. This discipline improves the quality of the testing and ensures that everyone involved has the same understanding of what is intended. Starting with objectives and scope for a test will make the planning easier. The tests should not be too ambitious, especially the first ones: only realistic goals should be set.

Reasonable timescales should be set for testing.

8.3.2 Planning and Conducting a Test

Planning a test:

• reduces the time and effort involved;
• enables more and better results to be achieved in fewer tests.

No test is ever a failure because, however badly it may seem to have gone, lessons can still be learnt from it. However, it should be remembered that if a test is not planned properly, it could actually create a disaster.
Live tests especially could create a disaster if not planned properly because they use real people and real resources in real conditions, probably during normal working hours. Live tests should only be considered after the BCP has been tested in full and all Recovery Team members fully trained, and even then simulation of a live test is safer than a truly live test. The worst way to test a Plan is to turn off the power suddenly, for example, and tell people to exercise their Recovery Plans as the interruption and delay to normal work could well become a disaster in itself.

The results of each test should be recorded to identify:

- what happened;
- what was tested successfully; and
- what needs to be changed.

If a test indicates that the BCP needs to be changed, the change should be made and the test repeated until all aspects are completed satisfactorily.

When all the components have been tested satisfactorily, the whole BCP is ready for testing. It should not be assumed that because the components work individually there is no need to test the whole BCP. Putting it all together may reveal problems which did not show up in lower level testing.

When preparing for testing, the participants should be given all the information and instruction they need.
8.4 TRAINING THE RECOVERY TEAMS

8.4.1 Initial Training

It should be remembered that every test also trains the participants. If the full Recovery Teams are not used in each test, the participants should be rotated so that they all gain equal experience.

At the end of the testing phase, further training and experience requirements should be identified. The Recovery Team Leaders should be consulted for their opinions as they should have the best understanding of the present abilities of their Team members.

A training programme should be drawn up in conjunction with the Recovery Team Leaders, including:

• the training method to be used:
  - walkthrough session;
  - scenario workshop; or
  - live test simulation; and

• the timetable.

In addition, Recovery Team Leaders should sometimes:

• give their deputies the opportunity to run the Teams as if the Leaders were absent; and

• act as observers for the training organiser.

8.4.2 Refresher Training

After the initial training a regular refresher programme should be set up. Refresher training should take place at least annually and include everyone.

If major changes are made to the BCP, additional training may be needed immediately rather than waiting for the next regular session.
8.5 Exercise Methods

Apart from live tests of the BCP, which are not generally recommended, there are other exercise methods which can be used for training as well as testing.

The three most effective methods are:

- walkthrough session;
- scenario workshop; or
- simulation of a live test.

8.5.1 Walkthrough Session

For a walkthrough session, the participants sit round a table, each with a copy of the BCP (or appropriate part of the BCP), and 'walk' through it by reading and discussing each part in sequence.

Participants should be:

- the key staff in the operation concerned and its Recovery Team;
- other staff who are knowledgeable about the operation and the way it fits into the organisation.

Walkthrough sessions should be conducted in a quiet place without interruption because the objective is to identify any weaknesses, errors and omissions by allowing participants' thoughts to flow freely as they go through the Plan. The only limit on discussion is that the whole part must be read to the end.

All components of the BCP should first be tested using this method as it is highly likely to identify changes needed. One good walkthrough per component is usually sufficient if the suggested changes are then reviewed and agreed by a few of the testers.

A suitable BCP component for testing using this method would be the complete Plan for one Recovery Team. Links with other Teams should be noted and raised during their walkthroughs.
8.5.2 **Scenario Workshop**

This is similar to a walkthrough except that a scenario is devised before the workshop, and at least the key members of the Recovery Teams must be involved, although it is preferable to include whole Teams.

Scenarios should be designed:

- around the actual conditions of the premises and its operations;
- to introduce any possible disaster in a realistic way;
- to give a good testing of the Plan;
- to include developments that would usually occur during a disaster, for example, changes in safety conditions delaying return to the premises.

Participants should sit round a table in a quiet place without interruption with their copies of the BCP (or appropriate part of the BCP), but instead of reading through the whole BCP, they should role-play their participation in the scenario. As they do so, they should say aloud what they are thinking and doing. The objective is to identify errors, omissions and weaknesses, and to establish whether the Plan performs as intended.

For this method to be effective, participants must:

- accept the scenario at face value;
- become fully involved in the role play; and
- voice all their thoughts and imagined actions. Brief interruptions to a participant’s spoken thoughts and actions are permitted if other participants have constructive comments or questions.

As the scenario progresses the lead participant(s) may change as appropriate to the timescale of the Plan, particularly if the whole BCP is being tested rather than one Recovery Team’s Plan. Participants need to be aware of this possibility so that it happens smoothly in the right places.
The Role of the Workshop Co-ordinator

The Business Continuity Officer or someone fully familiar with the BCP should act as Workshop Co-ordinator and:

• present the scenario;
• observe how the Plan performs;
• note any points that arise;
• generally keep the exercise on course;
• note the results of any decisions and actions that need to be completed by particular times in the scenario;
• prompt any change of lead participant(s) as the scenario develops, if appropriate.

Two problems may arise which the Co-ordinator must correct:

• participants may forget the Plan and invent their own course of action. In this case the Co-ordinator must bring them back to the Plan;
• some discussion may be constructive, but it must not be allowed to become general and interrupt the role play.

Working through the Scenario

The Co-ordinator:

• gives a short briefing to explain the purpose of the workshop;
• reads out the prepared scenario;
• gives a copy to each participant; and
• starts the exercise by saying ‘The scenario time is now x o’clock. Who does what?’

If the scenario has developments, the Co-ordinator should interrupt the role-play at the appropriate times to read them out. Although the BCP covers days, the workshop will of necessity be limited to a few hours. The Co-ordinator can progress the scenario time by interrupting to say ‘The time is now y o’clock.’

A sample scenario is included at the end of this section.
8.5.3 Simulation of a Live Test

This should:

- be held outside normal working hours so that resources can be used without affecting normal operations;
- involve the use of the planned and contracted contingencies if this is practical;
- relocate some staff to another site if appropriate; and
- be as near to real life as possible so that all aspects of the BCP, including contingencies, are tested.

Because it is a test, some shortcuts may be taken, such as sending only a token number of people to the contingency site, or doing only token amounts of work to prove that the operation has been successfully recovered. However, even if shortcuts are used it must still be possible at the end of the test to conclude that all aspects of the BCP are effective.

A simulation of a live test, perhaps more than the other methods, needs to be carefully planned to:

- ensure the testing is thorough;
- avoid confusion when things go wrong; and
- prevent any disruption to the real operations.
8.6

**BCP MAINTENANCE**

8.6.1

**Incorporating Changes**

Business Continuity Planning is concerned with the effects that changes have on the BCP. Change can:

- range from physical alterations to the premises to reorganisation of, or within, the business units; and
- be fast or slow, large or small scale.

Some changes have an obvious effect, for example:

- if an operation ceases to exist, there is, therefore, no further need to recover it;
- if a new operation is introduced, it may need to be recovered;
- if an operation alters, its requirements for recovery may also change;
- if there are changes in the immediate neighbourhood, such as building work or road widening, there may be implications for the safety and security of the premises which need to be incorporated into the BCP.

Other changes and their implications for the BCP may not be so obvious. For example, linking the personal computers in the premises to a File Server in a Local Area Network would probably cause a change in the requirements for recovery, and if there is a contract for office accommodation this may also need revision.

If the BCP is to remain effective it must be kept up to date. Obvious major changes should prompt an immediate check for the need to update the BCP. If the alterations needed are more than minor they should be made in step with the changes causing them.

The best way to ensure that a BCP is up to date is to test it, train staff in how to use it, and review it regularly.
8.6.2 Further Testing and Training

Changes to the BCP usually require further testing and training. This could be delayed until the next planned session if the change is minimal and a note should be made to examine the effect of the change in the next training/testing session.

8.6.3 Reviewing the BCP

The BCP should be reviewed with each business unit’s manager to identify changes and check that the business unit’s recovery requirements are still valid. Such reviews should be carried out at specified intervals, usually annually but more often if the rate of change is high. Keep a record of review dates.

Remember that whenever the BCP is amended, the latest version must be distributed to all holders and the old versions destroyed. Successful recovery could be jeopardised if anyone is working to an older version.
8.7 WHAT SHOULD YOU DO?

1. Ensure that everyone is aware of the BCP development project and that the level of awareness is maintained.

2. Test the drafted Plans as soon as practicable using a planned programme.

3. Amend any errors and omissions identified by testing, then re-test the Plans.

4. Complete the testing within a reasonable timescale.

5. In conjunction with the Recovery Team Leaders, plan a programme of training to ensure that everyone involved in Business Continuity Planning has adequate training and experience.

6. Complete the initial training within a reasonable timescale.

7. Set up and timetable a programme of refresher training.

8. Set up and timetable a programme to review the BCP for the effects of changes in the premises and/or its operations.

9. Be prepared to identify and make immediate changes to the BCP resulting from major changes in the property and/or its operations.

10. Test all changes to the BCP.

11. Make sure:
    • everyone has the latest version of the BCP; and
    • old versions are destroyed.
ANNEX 8/1: SAMPLE SCENARIO

This is an example of a scenario referred to in section TEST 8.5.2 under Scenario Workshop. This particular scenario was used for one office of a large corporation on the south coast of Britain.

Workshop Background

Choice - Fire is excluded because it is a common cause and therefore is too readily expected and understood. This scenario uses the presence of the railway line on the raised embankment at the northern boundary of the site for an accidental tanker spillage.

The scenario development does not provide clear concise information to allow anyone to know when normal working can resume. It will specially test the BCT's judgement about gathering helpful information and taking a view that the building will not be usable for three working days at least.

After one hour the telephones should have been redirected.

By late afternoon the BCP should be fully invoked. Hopefully the BCT will reach that decision before the final Scenario Update.

The scenario should prompt thoughts on what might need to be done after the police cordon has been removed to make the building safe to re-enter.

It will enable more than the first 48 hours, which the BCP specifically addresses, to be covered by the BCT but only by touching lightly on the post-48 hour period.

Workshop Objectives

The workshop has two objectives:

1. To familiarise the key players with their Plans and with the processes involved in reacting to a disaster situation.

2. To check the accuracy and suitability of the Plans by giving the key players the opportunity to comment as the role playing proceeds.

In short, every exercise of a BCP has elements of both testing and training even when specifically targeted at only one of them.
Conduct

The workshop co-ordinator will:

- explain the objectives, briefly;
- explain the conduct, briefly;
- read aloud the scenario and hand out copies;
- at the appropriate times during the role playing, read out three successive scenario updates, handing out copies to participants.

After each scenario reading the players will be asked, “Now, who does what?”

The appropriate key player is expected to role-play by stating aloud his actions and thoughts, even his reasons if he wishes. Other players will take the lead at their appropriate points in the scenario development.

At any time other players may interrupt with questions and comments. The co-ordinator will allow some discussion where it is pertinent and contributes to the exercise.

At other times the co-ordinator will keep the players to their Plans and the scenario.

Duration

The role-playing should last about two hours, with discussion of the event taking up to another hour. The total time taken, however, may vary depending on how involved the players become and how much discussion arises.
The Scenario

Time - 10:00 a.m. Monday morning, June. Weather sunny and warm, no cloud or winds forecast.

Event - From a passing train, two tankers derail and topple down this side of the embankment. One crashes through the fence and damages the fronts of parked cars, the other lies angled down the slope, still connected to the first. Both lie with their tops downhill and liquid is leaking from the top hatch of the first.

10:15 Fire Service arrives on the far side of tracks. Company employees in car park back away complaining of stinging sensation in air.

10:30 Police begin to arrive both sides of tracks, summoned by fire fighters who have read the Haz. Chem. symbols on the derailed tankers, and order immediate evacuation of all adjacent property. The Department’s staff are not allowed into car park to remove vehicles.

10:55 The Department’s emergency evacuation completed. Police exclusion zone extends a quarter of a mile in each direction.

Now, who does what?
First Scenario Update

11:30 Premises Manager informs BCT that contact has been established with the police. Premises Manager has learned that:

- ambient temperature is vaporising the escaped liquid;
- the liquid and its gas are not flammable but are toxic, irritating and slightly heavier than air;
- there is a lack of wind to disperse the gas which is lying in invisible clouds on the ground and it is thought that it could be up to 3 metres deep. Some of it will obviously roll down the gradient to the sea and there be dispersed;
- the police have no idea when the emergency will be over.

11:40 BCT advised that Premises Manager established contact with a Rail spokesman who is unable to indicate when the emergency will be over. When pressed, he stressed the dangerous nature of the gas to the RailTrack workmen and that it is highly unlikely to be cleared before midnight.

End of first update, please carry on.

Second Scenario Update

2:30 p.m. The Premises Manager succeeds, via the Rail spokesman, in establishing contact with a RailTrack official on their emergency engineering team. The official repeats the problems of working with dangerous cargoes, and points out the risk that the leakage could increase when they try to move either tanker: “The top hatch could pop fully open and spill a lot of liquid before we can close it, if we can close it.”

When pressed he says, “Look, don’t quote me because nobody really knows yet but my guess, and it’s purely a guess, is that we won’t get the tankers out of here before tomorrow afternoon.”

End of second update, please carry on.
Third and Last Scenario Update

6:00 p.m. The Premises Manager learns from the RailTrack engineering team official that lifting gear and breathing apparatus will not be assembled and on site before 6:00 a.m. and the actual start could be a few hours later.

Visual inspection from a safe distance suggests that it could take 10 hours from start to towing the tankers away. In the meantime they are trying to work out a method to prevent the top hatches from opening any further.

End of last update, please carry on.
9.0 INTERIM BUSINESS CONTINUITY PLANS

9.1 About this Section

9.2 Purpose of an Interim Business Continuity Plan

9.3 Developing an Interim Business Continuity Plan

9.4 What Should You Do?

Annex 9/1 Example of an Interim Business Continuity Plan
9.0 INTERIM BUSINESS CONTINUITY PLANS

9.1 ABOUT THIS SECTION

This section explains:

- the purpose of an Interim Business Continuity Plan (BCP); and
- how to develop an Interim Plan.

An example of an Interim Plan is given at the Annex to this section.

9.1.1 Key Points

The key points to note for Interim Plans are:

- an Interim Plan should only be regarded as a temporary measure and not as a substitute for a full BCP;
- Interim Plans should be devised by one or two senior managers;
- when devising an Interim Plan, senior managers should not spend more than three hours on establishing the main requirements.
9.2 PURPOSE OF AN INTERIM BUSINESS CONTINUITY PLAN

An Interim Plan offers limited protection whilst a full BCP is being developed. It should, however, only be devised for premises which are regarded as particularly vulnerable.

An Interim Plan should only be regarded as a temporary measure and not as a substitute for a full BCP. Because an Interim Plan is only intended to offer limited protection, very little time should be spent developing it.
9.3 DEVELOPING AN INTERIM BUSINESS CONTINUITY PLAN

Interim BCPs should be developed by one or two senior managers. To devise an effective Interim Plan, they should consider the following points, spending not more than three hours in total on the whole exercise:

- appointing a Business Continuity Team (BCT) to action the Interim Plan;
- establishing a procedure for calling out the BCT outside normal working hours;
- identifying the basic recovery requirements for the premises;
- identifying practical alternatives to replace essential operations when a disaster has happened;
- taking preventative measures to protect data, records and documents from the effects of a disaster;
- making sure that all members of the BCT have a copy of the Interim Plan and that they are fully briefed on its contents;
- making sure that copies of the Interim Plan are stored off-site where they can be easily retrieved if needed.

9.3.1 Business Continuity Team

BCTs should be appointed from mid to higher management and there should be enough members to ensure that at least two are available to act immediately, whatever the circumstances. They will be responsible for invoking the Interim Plans.

9.3.2 Call Out

A procedure for calling out the BCT outside normal working hours should be established. This could be done as follows:

- the security guard or duty keyholder is given the names and contact numbers of all members of the BCT;
- all members of the BCT have a list of each others’ names and contact numbers;
• the BCT and security guard/duty keyholder agree under what circumstances the BCT should be called out outside working hours; and

• the security guard/duty keyholder contacts a member of the BCT when the agreed circumstances arise, who, in turn, contacts the rest of the BCT.

9.3.3 Business Recovery Requirements

Basic business recovery requirements need to be identified. This can be done by:

• identifying essential operations carried out on the premises which need to restart as soon as possible after a disaster has happened, so that the services expected from the premises can continue as normal;

• establishing how soon the essential operations must restart after a disaster has happened; and

• identifying the minimum resources needed for the essential operations to restart.

All this information should be included in the Interim Plan so that it is immediately available to guide recovery actions.

9.3.4 Contingencies

Contingencies are practical alternatives which can be arranged in advance to replace essential operations. However, they should only be used for the purposes of the Interim Plan. These alternatives should be identified, their details included in the Interim Plan and be referred to at Task 9: Decision Process of the Annex to this section.

9.3.5 Preventative Measures

Data, records and documentation are items whose loss is devastating when a disaster take place. Preventative measures to protect them which can be put into place inexpensively and quickly should therefore be identified. Details of these preventative measures should be included in the Interim Plan and referred to at sub-section INT 9.5, Task 9: Decision Process of the Annex to this section.
9.3.6 **Familiarisation**

All members of the BCT, or at least the key members, should be fully briefed on the contents of the Interim Plan.

9.3.7 **Holding Copies of the Interim Business Continuity Plan**

Each member of the BCT should have a copy of the Interim Plan. Some copies should also be stored offsite where they can be easily retrieved if needed. If all copies of the Interim Plan are held on the premises, it may be impossible to retrieve them when a disaster happens.
9.4 WHAT SHOULD YOU DO?

1. Develop an Interim Plan if your premises are particularly vulnerable.

2. Appoint a BCT to invoke the Interim Plan.

3. Establish a procedure for calling out the BCT outside normal working hours.

4. Identify basic business recovery requirements.

5. Identify contingencies and preventative measures.

6. Make sure all members of the BCT:
   • are familiar with the content of the Interim Plan; and
   • have a copy of the Interim Plan.

7. Store some copies of the Interim Plan off-site.
ANNEX 9/1: EXAMPLE OF AN INTERIM BUSINESS CONTINUITY PLAN

The following example of an Interim Plan lists the tasks that should be carried out as soon as a disaster, or potential disaster, is discovered and/or an emergency evacuation of the premises has taken place. It contains guidance on:

- receiving notification of a disaster or potential disaster;
- staff and public safety;
- liaising with Departmental Security Officers;
- contacting the emergency services;
- calling out the Incident Control Team;
- deciding whether or not a disaster situation exists;
- calling out other members of the BCT and arranging the first meeting;
- invoking the Recovery Plan, liaising with Recovery Teams;
- arranging emergency premises and relocating to another site;
- ensuring that the security of the original premises is maintained;
- advising office services of any changes to their routine resulting from the incident;
- staff and news media communication; and
- monitoring the recovery process.

Other tasks can be added to the list if necessary, but any additions should be kept to an absolute minimum. Similarly, any of the tasks that are not appropriate can be ignored.
1. Receive Notification of the Disaster or Potential Disaster

Notification of a disaster or potential disaster may come from any source at any time. Obtain as much information as possible from the person giving the notification.

2. Give Priority to Staff and Public Safety

If the incident occurs during normal working hours, the first priority is the safety of staff, contractors, visitors and the public. Make sure that:

- everyone is accounted for;
- the emergency evacuation drill has been carried out, if necessary;
- first aiders or appointed persons attend to any casualties, if appropriate, and the Ambulance Service has been summoned.

3. Liaise with Departmental Security Officers

If the incident has security implications, liaise with Departmental Security Officers to make sure that security is not breached, removed or weakened as a consequence. Take their advice on any other security considerations.

4. Contact the Emergency Services

If necessary, check that the following emergency services have been summoned, as appropriate:

- Fire Service;
- Police; and
- Ambulance Service.

5. Call Out the Incident Control Team

Call out the Incident Control Team. Ask them for any information they can provide and share their Incident Control Room if necessary. (Sharing should be agreed beforehand when developing the Interim Plan.)
6 Decide whether or not a Disaster Situation Exists

Declare that a disaster situation exists immediately if it is one of those listed below and the impact will last longer than an acceptable period. If this is the case, ignore Task 9: Decision Process.

Disaster situations include:

- destruction or severe damage to the premises which makes it impossible to use, for example fire, flood, collapse, contamination. Seek clarification immediately if the information you have on the incident is unclear or insufficient;
- external events which prevent access to the premises, for example police cordon, emergency evacuation, adverse weather conditions;
- total loss of essential services, for example power, telephone, computers, heating and other environmental controls;
- other events which may make it dangerous for staff and/or the public to stay on the premises, for example discovery of asbestos.

7 Call Out Other Members of the Business Continuity Team

If the other members of the BCT are not present:

- contact them;
- advise them of the situation; and
- arrange to meet at a suitable place.

8 First Meeting of the Business Continuity Team

If the designated Team Leader and Deputy Leader of the BCT are not present, choose a Team Leader to take overall responsibility and co-ordinate action.
9 Decision Process

The BCT must decide whether or not to:

- declare that a disaster situation exists; and
- invoke the Recovery Plan.

To do this, the BCT should:

- seek advice immediately if the information on the incident is uncertain, unclear or insufficient;
- if the situation is a potential disaster, decide what the Maximum Acceptable Outage Time (MAOT) is. Give a realistic estimate of when the situation will return to normal and monitor the situation. If at any time it is likely that the MAOT will be exceeded, a disaster situation must be declared. The MAOT should not be extended because of information that the situation will return to normal soon after the MAOT is due to expire;
- assess the impact of the disaster on the business operations that are carried out on the premises. Note that a seemingly small disaster can have a much wider impact than expected, for example a fire in one part of the premises can cause smoke and water damage which affects other parts of the premises.

If the decision is taken to declare a disaster situation and invoke the Recovery Plan, remember that the Recovery Plan can be cancelled at any time if the situation does not prove to be a disaster.

10 Invocation of the Recovery Plan

To invoke the Recovery Plan:

- open a log of events and appoint a member of the BCT to maintain it
- record the following details in the log:
  - property lost, both personal and Departmental;
  - expenses incurred;
  - problems encountered; and
  - outline of the main events (not a detailed account);
• contact:
  - the Departmental Security Officer;
  - the Incident Control Team; and
  - other appropriate parties, for example other Departments, the Minister’s Private Secretary, and give them the following information as appropriate:
    - type, impact and time of the incident;
    - whether there have been any casualties;
    - where you can be reached; and
    - what support you need from them (see also Task 11: Arrange Emergency Premises below).

11 Arrange Emergency Premises

If it is likely that the original premises will be damaged to such an extent that it will impossible to use even part of them, find out if any space is available in neighbouring or associated premises. PACE can help you find alternative premises. Contact them to let them know how much space is required, working on the basis of 11 cubic metres per person to be accommodated.

12 Relocation to Another Site

If staff can be transferred to another site to resume business operations:

• inform all relocating staff as soon as possible:
  - when and where to meet;
  - what they should bring with them; and
  - how long they will be away; and

• arrange for any recovery material stored off-site to be collected and transported to the relocated staff.
Maintain Security of the Premises

Ensure that the security of the premises is not reduced or removed as a result of the disaster.

If staff are relocating to another site, the current level of alert should be established. Contact the Departmental Security Officer for further information.

Advise Office Services

Contact the cleaners and any other services which call at the premises on a regular basis, and advise them of any changes to their routine resulting from the disaster.

Staff Communication

Notify all staff and contractors about the disaster as quickly as possible, and inform them of relevant information regarding any temporary arrangements. Remember to notify switchboard operators, messengers and security guards.

News Media Communication

Remind everyone that they must not speak to the press, radio or television and that all enquiries should be referred to the Departmental Press Officer.

Operation Recovery Teams

Contact the Team Leaders or Deputies of the Recovery Teams to:

- brief them on the situation;
- advise them whether they should invoke their individual Recovery Plans; and
- confirm whether they will be relocated and, if so, to where.

Monitor the Recovery Process

Check that recovery is proceeding as expected at regular intervals. Take the necessary action to resolve any unforeseen problems which are delaying recovery.
10.0 INCIDENT CONTROL

10.1 ABOUT THIS SECTION
10.2 PURPOSE OF INCIDENT CONTROL
10.3 INCIDENT CONTROL TEAM
10.4 INCIDENT CONTROL TEAM ACTION
10.5 EMERGENCY PROCEDURES
10.6 ADDITIONAL CONSIDERATIONS
10.7 INCIDENT CONTROL MANUAL
10.8 INCIDENT CONTROL ROOM
10.9 DAMAGE ASSESSMENT AND SALVAGE
10.10 WHAT SHOULD YOU DO?

ANNEX 10/1 SAMPLE INCIDENT CONTROL PROCEDURES
10.0 INCIDENT CONTROL

10.1 ABOUT THIS SECTION

This section explains:

- the purpose of Incident Control;
- how to appoint an Incident Control Team (ICT);
- the actions an ICT need to take;
- how to compile an Incident Control Manual and Emergency Pack;
- how to set up an Incident Control Room;
- the emergency procedures required;
- factors to consider when devising emergency evacuation procedures;
- additional factors which Incident Control needs to address;
- procedures for damage assessment and salvage.

This information will help Departments which do not already have an Incident Control function. It can also be used by Departments who already have this function as a means of checking and improving their Plans.

A set of sample procedures for the ICT can be found at the end of this section.

10.1.1 Key Points

The key points to note for Incident Control are:

- Incident Control is about managing a physical crisis at the premises;
- speed is essential in dealing with an incident;
• the objectives of Incident Control, in order of importance, are:
  - to protect lives;
  - to prevent the incident from escalating to a disastrous level;
  - to contain any damage and reduce the impact; and
  - to make sure salvage and emergency repairs are started;

• the ICT should check that other emergency procedures have been followed if required.
10.2 **PURPOSE OF INCIDENT CONTROL**

For the purpose of this Guide, Incident Control is a method for dealing, at the premises, with the immediate physical effects of an actual or threatened disaster, for example fire or flood.

The incident itself may become disastrous in that it may:

- leave the premises unusable for more than a predetermined acceptable length of time; and/or
- prevent some or all of a business unit’s essential operations being carried out.

The seriousness of the effect of the incident could range from minor to major and the presence of an Incident Control function will reduce the likelihood of the BCP being invoked.

The most important objective of Incident Control is to ensure the preservation of life by:

- preventing injury;
- providing shelter; and
- evacuating the premises, if necessary.

Other objectives of Incident Control are to:

- prevent the incident from escalating into a disastrous event;
- reduce and control its effects; and
- make sure salvage and repairs are started at the earliest opportunity.

Incident Control does not replace the emergency services. If there is a threat of fire, or fire has broken out, the Fire Service must be called and Incident Control must work with or around them as the Fire Service permits.
Incident Control is the premises’ emergency response service in a crisis, and speed of reaction is essential. Incident Control must ensure that, as appropriate, the following take place:

• fire/emergency evacuation procedures;
• bomb search;
• calling the Emergency Services; and
• removal of valuable objects, if appropriate.

However, as the Teams responsible for these procedures must act without delay, they can do so independently without waiting for instructions from the ICT if circumstances warrant. The ICT must make a separate check that the Recovery Teams have acted. If there is only a threatening incident, for example if a piece of equipment has seriously overheated, full emergency procedures may not be necessary.

At appropriate points, the ICT should also check whether any necessary emergency procedure actions have been carried out.

The ICT should also make sure the premises remain secure during the incident and any subsequent recovery.

Other members of staff, visitors and the public should not be allowed to disturb those engaged in recovery, either physically or by telephone.

Incident Control deals with the physical effects of the incident. When the incident is over:

• Premises Management staff will:
  - deal with any damage which may have occurred to the premises;
  - inform landlords, neighbours, tenants or other leaseholders of the incident and damage, if necessary;
• the BCP will direct the continuity and recovery of operations.
10.3 INCIDENT CONTROL TEAM

The ICT consists of people who will carry out the Incident Control function. The ICT should have:

- a Team Leader;
- a Deputy Leader;
- enough members to ensure a minimum turnout in any circumstances;
- the authority to co-ordinate Incident Control on behalf of the Department;
- access to people with specific areas of responsibility and expertise as additional support, depending on the nature and size of the event;
- a team member assigned to liaise with and advise off-site services, including the emergency services, if the event requires their attendance.

10.3.1 Incident Control Team Members

Members of the ICT should:

- be quick-thinking people with good judgement and the ability to act quickly;
- live within a reasonable travel distance of the premises, and have their own transport if required to attend incidents outside normal office hours; and
- be volunteers.

Before confirming team membership, consideration should be given to any relevant conditions of employment or Trades Union agreements, for example concerning payment for being on call or called out or working unusual hours or conditions.

Because Incident Control deals with physical incidents at the premises, the Premises Manager should either be a member of the ICT or should co-operate closely with them. However, the Premises Manager should not be the Team Leader or Deputy Leader because there may be other demands on him/her during incidents.
Two or more premises which are close together may consider forming one combined ICT. This would give a wider choice of staff from which to choose the most suitable ICT members. Training, the Incident Control Room and facilities would also be more cost-effective as their costs would be divided between the participating premises.

10.3.2 Authority

The ICT must have the authority to take urgent decisions or actions which may cost money, for example hiring a salvage firm or equipment to secure the premises. Management should give the ICT guidance on this subject by setting a reasonable limit within which they may spend. This authority should be given to the ICT members individually, because they may have to act in crisis conditions. A lower spending limit could be set for individuals and a higher limit for any two ICT members acting together.

The ICT must also have authority to:

• order people to leave the premises; and
• request them to assist the ICT or with other emergency procedures, for example to check that an area is clear of people following evacuation, provided it is safe and reasonable to do so. See also sub-section IC 10.5.1 below.

10.3.3 Co-ordination

The actions of ICT members must be co-ordinated to prevent confusion and conflicting decisions. They must therefore maintain contact with each other at all times. Mobile telephones or radios and working from a central point (the Incident Control Room) will provide this mutual contact, and the Team Leader and/or Deputy will act as a focus to co-ordinate actions. If both the Team Leader and Deputy are absent, the Team must elect a leader at the earliest opportunity to take charge and co-ordinate actions.

If mobile telephones or radios are to be used, they should be tested throughout the premises to identify any reception ‘black spots’. Mobile telephones should be registered under the Access Overload Control (ACCOLC) Scheme which provides for priority access by registered cellphones if the network becomes overloaded in an emergency.
10.3.4 Liaison

The ICT will need to liaise with the Emergency Services and other external services which may be present. A nominated ICT member should make contact with the Emergency Services to:

- explain their role;
- advise where and how they and the Incident Control Room can be contacted;
- try to obtain similar information and co-operation from the Emergency Services.

If salvage engineers have been called in, the ICT will also need to liaise with them.

The ICT will need to work closely with the Premises Managers. If the Premises Managers are not members of the ICT, it may be appropriate to invite them to work from the Incident Control Room with the ICT. It may also be appropriate to invite the Business Continuity (BC) Team to make use of the Incident Control Room during the incident.

Contact with the Emergency Services and the Premises Manager should be made at the earliest opportunity.

10.3.5 Incident Control Team Call Out

A procedure should be devised and put in place for calling out the ICT, both during and outside working hours. Call Out should have a high priority as rapid action is needed when dealing with an incident. If the premises has a 24 hour security service, they should be given:

- a list of the circumstances in which the ICT is to be called out;
- instructions to call out any two ICT members, starting with the Leader and Deputy;
- a list of names and contact details of all ICT members, divided into those for normal working hours and those for outside normal working hours.
If there is no overnight presence on the premises, the keyholders could be responsible for calling out the ICT outside working hours. Consideration could be given to an on-call system whereby individuals rotate the duty of being available to deal with emergencies.

All ICT members should have a copy of the complete ICT list and contact details. The members contacted first should then contact the rest of the Team, but they should agree whom each will contact to avoid duplicated effort.

10.3.6 **Training the Incident Control Team**

The ICT should receive training, information and instructions. Suitable methods are the Scenario Workshop and the Simulation of a Live Test described in section TEST 8.5 of this Guide.

10.3.7 **Staff Notification**

If an incident occurs outside normal working hours it may be advisable to warn staff to keep away from the premises if this is decided to be appropriate. Notification of staff should not be a task for the ICT; they should only start the process. See *Contacting Other Staff* in section PLAN 7.5.7.
10.4 INCIDENT CONTROL TEAM ACTION

The possible causes of a disaster are too numerous and too unpredictable to anticipate, so the ICT must be prepared to deal with any kind of incident. This means that it must be reactive and act quickly. The action the ICT takes will also be dictated by the stage the incident has reached by the time they are called, either to:

- prevent the incident from escalating into a disastrous event if it is little more than a threat; or
- control the extent of potential damage if the escalation cannot be prevented.

The sequence of action the ICT should take when called out is described in the following sub-sections.

10.4.1 Assess the Situation

This should be done by:

- first hand inspection on the spot;
- obtaining opinions from the Premises Manager or other competent or reliable people, such as an electrician for an electrical incident or a plumber for a water or drainage incident.

If there is a threat of danger to life, action such as evacuation must be taken immediately. If security is of extreme importance at the premises, the ICT should consider whether the incident could be a cover for an attempt to penetrate security.

At the same time, the Incident Control Room (if there is one) should be opened and put into use.

10.4.2 Prevent the Incident from Escalating into a Disaster

If the incident is still little more than a threat, the ICT should take whatever practical action is appropriate and possible to prevent it from escalating. This could be as simple as summoning the Fire Service, plumbers, electricians or other services, or experts such as building engineers to advise.
10.4.3 Contain and Minimise the Damage

If the incident cannot be prevented the ICT should take practical action to contain and minimise the potential damage. For example if:

- a fire sets off alarms, the ICT should:
  - call the Fire Service if this is not done automatically;
  - obtain and spread waterproof sheets to prevent water damage; or

- there is a flood, they should arrange to move items above flood level or off the premises to a place of safety.

At appropriate points the ICT should also check whether any necessary emergency procedure actions have been carried out, for example:

- fire/emergency evacuation procedures;
- calling the Emergency Services;
- bomb search;
- removal of valuable objects; and
- call out of the BCT.

A typical sequence of events and actions involving the ICT is illustrated at IC 10.4.5.

Detailed emergency procedures are given in section IC 10.5.

10.4.4 Salvage and Repairs

After the crisis, the ICT should:

- consider calling in salvage experts to rescue items and/or stabilise their condition; and
- make sure the premises are safe, for example made weatherproof if windows or roofs have been damaged.
Typical Sequence of Events for the Incident Control Team

1. Incident
2. Call out Incident Control Team
3. Incident Control Room opened
4. Emergency services called
5. Effect of incident assessed
6. Human safety assured (e.g., evacuation)
7. Further preventative action
8. Mitigative action
9. Remedial action
10. Call out Business Continuity Team if needed
10.5  

**EMERGENCY PROCEDURES**

The ICT should ensure that, as a minimum, procedures for the following exist, and that people have been assigned and trained to action them:

- fire drill;
- emergency evacuation;
- bomb threat and search - see Home Office booklet *Bombs - Protecting People And Property, A Handbook For Managers And Security Officers*;
- first aid; and
- removal of valuable objects.

If any procedures need to be put into place, advice may be obtained from PACE.

Regular reviews with the police and Fire Service should improve procedures for emergency evacuation.

10.5.1  

**Fire Evacuation**

The following action is a basic guide. Comprehensive information about fire evacuation is contained in the PACE Fire Safety Guide.

Staff must be appointed with a responsibility for controlling evacuations, usually the Premises Managers. They are chiefly responsible for:

- the alarms;
- the preparation of procedures;
- conducting drills;
- ensuring that the building is cleared by appointing someone at the Assembly Point to collect information.
When preparing evacuation procedures it should be remembered that:

- people with physical disabilities may need help with evacuation;
- problems could arise from, for example:
  - seasonal conditions and temperature;
  - inclement weather; and
  - the time of day, for example the risk of staff dispersal at lunch time or staff returning from lunch going into the evacuated premises.

**Escape Routes**

Escape routes must:

- be chosen for each floor or area, to prevent congestion which could slow down the evacuation and lead to crowd-press injuries;
- all have an alternative in case the first is unusable or unsafe;
- not involve use of lifts, because they could fail, unless they have been given prior approval for this by the Fire Service and/or the relevant Enforcing Authority.

Escape routes will be identified in any Fire Certificate for the premises.

**Assembly Point**

A suitable safe Assembly Point (or Points) should be chosen where staff should gather when evacuated. It should:

- be far enough away from the premises to be:
  - out of danger; and
  - out of the way of the emergency services;
- have some means of communication with the ICT.

Staff should be instructed not to leave the Assembly Point until told to do so.
Alarms

It is advisable to have two alarms:

- the first alarm should be intermittent ringing; meaning ‘be ready to evacuate’;
- the second alarm should be continuous ringing, meaning ‘evacuate’.

When the first alarm sounds, Premises Management staff should check for false alarms and other correctable conditions such as small fires which can be quickly extinguished or overheated equipment which can be switched off.

Evacuation Checks

It is important to be sure that everyone has been evacuated from the premises because the Fire Service will need to know immediately if they need to enter specifically to rescue anyone. Working from a headcount of those evacuated is not reliable because:

- an accurate record of everyone who was inside the premises may not be readily available;
- people may move away from the premises or become separated from their colleagues.

A quicker and safer method is to ‘sweep’ each floor or area to find anyone who is left behind or not aware that evacuation is under way. The sweep should be done by Floor/Area Fire Wardens normally present on their floor or area and assigned to be the last ones out.

Floor/Area Fire Wardens should:

- quickly check all offices, toilets and other closed rooms to make sure no one is left in them;
- at the Assembly Point, confirm evacuation of their area, for example by ticking a list or hanging a numbered tag on a matching numbered hook on a board.
• have the authority to:
  - order people to leave;
  - instruct them how to leave;
• have deputies to cover for absences.

**Evacuation Drills**

Staff should be given clear and concise instructions on evacuation, and drills should be performed regularly. When the full alarm sounds, staff:

• must not return to their desks;
• should leave the premises immediately using the appropriate escape route or as directed by a Floor/Area Fire Warden; and
• must not take with them bulky or awkward objects which could block the escape route.

Each drill should be timed to establish how long it takes to clear the premises. Problems which delay evacuation should be identified and corrected.

**10.5.2 Bomb Evacuation**

The fire evacuation procedures should be used as the basis for evacuation for bomb threat, but the following factors should also be considered.

After evacuation staff should not be exposed to danger from the bomb blast or subsequent damage to the premises. This can only be determined at the time of the incident and the evacuation instructions should be altered accordingly. Floor/Area Fire Wardens could help to reorganise escape routes.
Depending on the circumstances (for example lack of time, lack of safe escape routes, unknown location of bomb), it may be advisable to "evacuate inwards" to a safer part of the premises. Any internal Assembly Point:

- should be chosen so that people there cannot be:
  - exposed to bomb blast; or
  - hurt by subsequent damage to the premises, for example flying glass or collapsing walls or floors;

- must have an exit which will remain safe so that staff cannot be trapped.

A structural engineer should be consulted for advice on the choice of an internal Assembly Point. (Note: It may not always be possible to find one.)
10.6 ADDITIONAL CONSIDERATIONS

When setting up an Incident Control function, the following need to be considered:

10.6.1 Multi-tenancy Occupation

If the premises are occupied by more than one Department, the lease and the Memorandum of the Terms of Occupation (MOTO) need to be checked for responsibilities. The holder normally has responsibility for Incident Control. If the premises has non-Government tenants, the landlord or agent may have this responsibility. The Departments should be satisfied that Incident Control is in place and, if not, the ‘house committee’ and/or landlord should consider and assign the responsibility.

10.6.2 News Media

If the press arrive during an incident they should be referred to the Departmental Press Officer.

Full details of the incident should be reported to the Departmental Press Officer.

If a severe disruption has occurred a Press Officer will be sent to the site. Initial press reports are often inaccurate or exaggerated and, for that reason, if approached by the media, staff should not:

- make statements without approval;
- divulge any information other than simple confirmation of the incident which has occurred;
- speculate;
- give out casualty names until the police have informed the next of kin.

If considered preferable, Departments may wish to consider instructing their staff to refer all media approaches to their Press Office.
10.6.3 Maintenance Contracts

The Facilities Management/Premises Management contracts should be examined to check whether call-out arrangements exist for specialists such as electricians, glaziers and plumbers. If not, consider inserting this into the contracts.
10.7

**INCIDENT CONTROL MANUAL**

A manual should be produced for the guidance of the ICT. Each member should have a copy. It should contain:

- callout information;
- Incident Control procedures;
- reference material such as:
  - plans of the building and its services, showing the main isolation points;
  - lists of experts who can be consulted urgently or summoned to give advice;
  - lists of repair services such as electricians, glaziers, plumbers, lift engineers.

A sample of procedures for Incident Control can be found in the Annex at the end of this section. See also sub-section IC 10.9, Damage Assessment and Salvage.

10.7.1

**Emergency Pack**

Consideration should also be given to compiling an emergency pack for use in emergency conditions, with a duplicate kept off-site as backup in case the original is inaccessible. Some of the items in the pack may duplicate the information in the Incident Control Manual, but would be kept loose for quick, easy reference. The pack could contain, for example:

- copies of the BCP;
- copies of the Incident Control manual;
- plans of the building and its services;
- lists of experts who can be urgently consulted for advice;
- lists of repair services such as electricians, glaziers, plumbers, lift engineers;
copies of useful documentation and recorded information, for example:

- Fire Certificate for the premises;
- COSHH Register;
- premises Asbestos Register;
- premises Health and Safety file;
- premises Operation and Maintenance manuals;
- Information and Press Officers' Directory;
- telephone and Government directories.
INCIDENT CONTROL ROOM

This is a ‘Command Centre’ for the ICT to use. The facility chosen should be appropriate to the size of the anticipated operation. It should contain facilities for use during an incident, at least some desks, chairs and telephones, and ideally:

- one or two separate meeting rooms;
- white boards on the walls with a supply of pens;
- mobile telephones ready for immediate use, or hand-held radios;
- direct line telephones;
- connections to the Government Telephone Service (GTN);
- fax and photocopying machines;
- hard hats, coveralls, boots, goggles, high visibility jackets/tabards and other protective clothing.

A member of the ICT should be assigned to be responsible for the maintenance of any equipment in the Incident Control Room.

The Incident Control Room should be:

- far enough away from the premises to be unaffected by the incident; but
- close enough to be convenient to allow quick access to the premises.

However, it may be more convenient to use a room on the premises if the premises are safe to enter at the time of the incident. More than one location should be nominated for the Incident Control Room in case the preferred one is not available.

An Incident Control Room is expensive to set up for occasional use. If there are two premises close together, each could consider providing a room to be made available immediately for use as the other’s Incident Control Room. In this case, procedures for access out of hours would need to be arranged. If security problems can be overcome, a similar arrangement could be considered with a nearby non-governmental organisation.
An alternative to an Incident Control Room is to use a hotel room. This may be unsatisfactory because:

- it is unlikely to have all the required facilities available on demand and may only be suitable as a place to meet with a telephone; and

- the delay in obtaining a suitable hotel room may not be acceptable.

However, a hotel may be able to offer a fully equipped meeting room with several direct telephone lines. This alternative should be carefully considered before choosing it.

Another alternative is to acquire and equip a portable building. It would need to be located where it would not be affected by an incident at the premises, but, again, it is an expensive solution for occasional use.
10.9  DAMAGE ASSESSMENT AND SALVAGE

If a fire, flood, explosion or impact has occurred, damage assessment should be carried out to determine the extent of the problem and the corrective action needed, including salvage.

10.9.1  Damage Assessment of the Premises

When access to the premises has been declared safe, the ICT should:

- obtain as full details as possible of the extent of the damage from Emergency Services personnel on site;
- make sure the managers or deputies of the affected business unit(s), for example Computing, are available;
- prevent anyone from entering the premises until their reason for doing so is clear and understood, for example to assess the damage, assess the level of assistance required or retrieve critical information;
- ensure that findings are recorded;
- wear protective clothing, for example hard hats, coveralls, gloves, boots, high visibility jackets or tabards;
- only enter the premises when accompanied, or after telling someone outside when they are going in and when they come out again;
- examine affected key area(s) in relation to business requirements, for example computer and communications rooms, office areas;
- accompany the relevant business unit manager to assess the damage in a particular area;
- identify and protect any evidence of deliberate damage;
- shut off water, gas and electricity supplies;
• ensure the premises are secure:
  - strictly control who enters the premises and what is removed;
  - take additional security measures and/or deploy extra staff to maintain security levels;
• record actions taken and equipment removed to prevent further losses and possible theft.

10.9.2 Reclamation Processes

The following issues should be taken into consideration and the time required for reinstatement assessed, depending on the severity of the incident. Professional advice will probably be required.

**Explosion**

If an explosion has occurred, checks should be made for:

• contamination;
• dust;
• debris;
• glass shards; and
• unstable working environment and structure.

**Fire**

If a fire has occurred, checks should be made for:

• need for dehumidification;
• smoke contamination;
• need for deodorisation;
• unstable working environment and structure.
Flood

If a flood has occurred, checks should be made for:

- need for dehumidification or drying;
- contamination: sewage etc;
- need for deodorisation;
- safety of electrical installations.

Computer and Communication Rooms

The ICT should:

- obtain immediate expert advice from salvage engineers and computer and communications equipment manufacturers or suppliers;
- ensure all power is off, including Uninterruptable Power Supplies to protect wet or contaminated equipment from further damage;
- not switch equipment on to see if it is operable, as this could cause further damage.

Damage Assessment of the Assets

Specific items for assessment are:

- computer equipment - the Computing business unit manager should assist the ICT to assess the condition of computer equipment.

- data - the ICT should:
  - examine the storage (probably a fire resistant safe);
  - ensure access to the storage is possible;
  - if necessary and possible, remove the safe from the premises;
  - examine the contents and assess the condition of the data in relation to its importance;
- if necessary, obtain specialist help to remove dust and smoke;
- if the safe cannot be opened, contact the safe suppliers.

- paper documents - as initial handling determines the degree of success of recovery of paper documents, the ICT should identify critical documents and:
  - seal the documents to prevent uncontrolled drying by wrapping them in cling film or plastic bags;
  - store the sealed documents in archive boxes;
  - freeze the documents to prevent mould growth and protect them from damage while handling. A commercial frozen food trailer could be rented if necessary;
  - remove from the premises all critical documents nominated as Priority Salvage;
  - record where the documents were originally located;

- valuable objects - if unique archives, works of art or similar items are on the premises, these should also be examined. Expert advice and assistance should be obtained before moving or handling them if there is any possibility that this would cause further damage.

10.9.4 Salvage Considerations

A salvage operation is likely to require more time and staff than anticipated. It may not be worth the effort to salvage many of the items and documents. Departments should decide exactly what is to be retrieved, and priority lists for retrieval should then be prepared. During the salvage operation quick, on-the-spot decisions are likely to be needed.
10.10  WHAT SHOULD YOU DO?

1. Identify your Department’s responsibilities, if any, for Incident Control.

2. Review any existing Incident Control arrangements.

3. Encourage the creation of an Incident Control function.

4. Investigate the possibility of forming a joint Incident Control function with other nearby premises.

5. Appoint the ICT.

6. Write the procedures for callout of the ICT.

7. Write the emergency procedures for the ICT, including advice about damage assessment and salvage from section IC 10.9. See Annex 10/1 for sample procedures.


9. Provide training, information and instructions for the ICT.

10. Consider and cost options for the Incident Control Room. Seek approval for the budget.

11. Equip the Incident Control Room and appoint someone to maintain the equipment in it.

12. Seek expert advice where needed, for example building engineers, plumbers etc.
ANNEX 10/1: SAMPLE INCIDENT CONTROL PROCEDURES

1. When notified of an incident, establish:
   - the nature of the incident (briefly);
   - whether evacuation has taken place;
   - which other ICT members have been notified;
   - the person giving the notification;
   - the time of the notification.

2. Contact one other member of the ICT. Decide who will:
   - go to the scene immediately - if you are this person, go to Step 3;
   - call out the rest of the Team and open the Incident Control Room - if you are this person, go to Steps 6, 7 or 8 as appropriate.

3. At the scene, assess the situation. Find out:
   - if it is a bomb threat. If so, follow the bomb threat procedures, including evacuation, if appropriate;
   - if there is risk of personal injury. If so:
     - call the Ambulance Service or First Aiders;
     - do not endanger yourself or allow anyone else to endanger themselves;
     - keep other people away from the premises;
     - evacuate people from the premises according to the Fire Evacuation Procedures;
   - if it is a fire, whether the Fire Service has been called;
   - whether the situation can be prevented from escalating into a disaster. If:
     - it cannot, go to Step 5;
     - it can, go to Step 4.
4. If the incident can be prevented from escalating into a disaster, consider its cause and what preventative action can be taken, for example:

- using a fire extinguisher to put out a small fire;
- calling the police to deal with intruders or vandals then trying to distract them from causing further damage (without endangering yourself);
- calling out:
  - a contracted service engineer to correct a fault in, for example, the lifts, electrical equipment, plumbing, drainage, heating;
  - a structural engineer;
  - those responsible for the removal of valuable objects.

5. If the incident cannot be prevented from escalating into a disaster:

- consider what can be done to contain the incident and to minimise damage, for example:
  - calling the Fire Service;
  - closing fireproof doors;
  - spreading waterproof sheets over valuable objects or equipment;
  - moving valuable objects above flood level or off the premises (call out those responsible for Artefact Removal Procedures);
  - calling salvage experts.

Now go to Step 9.

6. Contact the other Team members and send:

- some to the Incident Control Room; and
- some to the scene of the incident.

Do not waste time if Team members do not answer their telephone.
7. Go to the Incident Control Room.

8. At the Incident Control Room:

- the first Team member to arrive should:
  - open the Incident Control Room;
  - answer and record incoming telephone calls;
  - try to contact Team members who are still missing;
  - check mobile telephones or radios are in working order (batteries charged, dial tone received, etc) if appropriate;

- the next Team member to arrive should distribute the mobile telephones or radios to Team members at the incident scene;

- retrieve the copies of documentation and recorded information which may be needed from the Emergency Pack, for example:
  - building plans;
  - the Asbestos Register;
  - contact lists;
  - Fire Certificate;

- assign one Team member to open a log and record important information, occurrences and/or instructions received from the Team members at the scene;

- carry out any instructions received from the Team at the scene;

- advise the Business Continuity Team of the situation;

- inform:
  - other occupiers of the premises;
  - management and other staff.
9. After the crisis phase of the disaster has passed:

- ensure the security of the site is maintained, especially if the conditions are dangerous;

- call out:
  - contractors to repair minor damage, for example to weatherproof the building, fix broken pipes or board up broken windows;
  - salvage experts to retrieve documents and equipment;
  - a structural engineer to assess the safety of the premises.
**Notification of an incident**

Establish:
- nature of incident (briefly);
- whether evacuation has taken place;
- which other ICT members have been notified;
- person giving notification;
- time of notification.

**The person at the scene**

At the scene, assess the situation.
Follow emergency procedures depending on the cause.

**Bomb threat**
Follow the bomb threat procedures, including evacuation, if appropriate.

**Risk of personal injury**
- call the Ambulance Service or First Aiders;
- do not endanger yourself or allow anyone else to endanger themselves;
- keep other people away from the premises;
- evacuate premises according to the Fire Evacuation Procedures.

**Fire**
Find out if the Fire Service has been called.

**Can the situation be prevented from escalating into a disaster?**

- Yes
  - Take action to contain incident and minimise damage, for example:
    - call Fire Service;
    - close fireproof doors;
    - spread waterproof sheets over valuable objects or equipment;
    - move valuable objects above flood level or off premises;
    - call salvage experts.

- No
  - Take preventative action appropriate to cause of incident, for example:
    - use fire extinguisher to put out a small fire;
    - call the police to deal with intruders or vandals then try to distract them from causing further damage;
    - call out:
      - contracted service engineer to correct fault;
      - structural engineer;
      - those responsible for removal of valuable objects.

**The person who will call out the rest of the Team and open the Incident Control Room**

Contact one other member of the ICT. Decide who will:
- go to the scene immediately;
- call out the rest of the Team and open the Incident Control Room.

**Open Incident Control Room**

At Incident Control Room:
- answer and record incoming telephone calls;
- try to contact Team members who are still missing;
- check mobile telephones or radios are in working order;
- distribute mobile telephones or radios to Team members at incident scene;
- retrieve documentation and recorded information from the Emergency Pack;
- assign one Team member to open log and record important information, occurrences and/or instructions received from the Team members at scene;
- carry out any instructions received from Team at scene;
- advise Business Continuity Team of situation;
- inform:
  - other occupiers of premises;
  - management and other staff.

**After crisis phase of disaster has passed:**
- ensure security of site is maintained, especially if conditions are dangerous;
- call out:
  - contractors to repair minor damage;
  - salvage experts to retrieve documents and equipment;
  - structural engineer to assess safety of premises.