Controlling & Auditing Information System

Business Continuity Planning

Prepared by:

Basuki Rahmad, Dr, CISA, CISM

2011

TABLE OF CONTENTS

1. BUSINESS CONTINUITY 1

1.1 Background 1

1.2 Business continuity planning 1

1.3 The problem 2

1.4 This module 2

2. AN APPROACH TO BUSINESS CONTINUITY PLANNING 3

2.1 Contingency and continuity planning 3

2.2 The continuity planning process 3

3. PRELIMINARY WORK 6

3.1 Top management commitment 6

3.2 The survey 6

4. THE BUSINESS IMPACT REVIEW 8

4.1 Objectives 8

4.2 Business impact review 8

4.3 Risk reduction measures 10

4.4 Reporting to management 10

5. RECOVERY STRATEGY DEFINITION 12

5.1 Disaster prevention 12

5.2 Backup, recovery and media storage 13

5.3 Non-technical options 15

5.4 Technical options for recovery 17

5.5 Reporting to management 18

6. DEVELOPING THE BUSINESS CONTINUITY PLAN 20

6.1 Levels of business disruption 20

6.2 Sections of a continuity plan 21

6.3 Supporting requirements 24

7. TRAINING, TESTING AND UPDATING 27

7.1 Training 27

7.2 Testing the plan 28

7.3 Evaluating the results and updating the plan 30

8. AUDIT CONSIDERATIONS 32

APPENDIX 1: CASE STUDIES 36

APPENDIX 2: CONTINUITY PLAN PRO-FORMA 54

1. Business continuity

1.1 Background

Over the past 20 years government organisations have come to rely increasingly on the availability and correct operation of their computer systems in order to discharge their statutory obligations. Computer systems often play an important role in such diverse activities as the assessment and collection of taxes and customs revenues; the payment of state pensions and social security benefits; and in processing national statistics (births, deaths, crime, diseases, etc). Indeed many activities could not now be carried out effectively - if at all - without the support of computers.

Loss of power, industrial action, fire, malicious damage can all have disastrous effects on computer systems. As the recent spate of bomb blasts in London, and also that at the World trade centre in New York (case study number 2, Annex 1) illustrate, it may take an organisation many weeks to resume effective business operations if they do not have a workable business continuity plan in place.

1.2 Business continuity planning

Business continuity planning is about planning to recover key business processes following a disaster. Disasters are not just restricted to fire, flood and other causes of damage to property; they can equally result from more mundane problems, such as strikes, or hardware or software malfunctions. And although restoring computer processing is an important milestone on the road to recovery, other equally important problems often need to be resolved. For example, it may be necessary to be able write cheques to ensure that employees and suppliers continue to be paid; this in turn may require the ability to maintain some form of accounts clerically.

The overall objective of producing and maintaining a business continuity plan is to .....

maintain the integrity of the organisation's data together with an operational service and processing facilities and, if necessary, provide a temporary or restricted service until normal services can be resumed.

Overall, effective continuity planning will require a range of skills, together with an understanding of the:

- business environment and its objectives and strategies;
- full range of risks that face the business, and the most cost-effective options for managing them;
- people, communications and other support services on which the business systems rely.

The losses to an organisation that result from the unavailability of their business systems increase with time. The objective of business continuity planning is to make

plans that are designed to reduce downtime - and hence loss to the business - to a minimum. Plans therefore need to be detailed and leave as few decisions as possible until after the event. They need to spell out the specific actions must be taken in order to restore business key business activities in a variety of disaster scenarios.

1.3 The problem

Business continuity planning is an aspect of corporate security and as such is a management problem. In practice it is rarely taken it seriously because top management :-

- consider it too expensive - probably the most frequently encountered reason;
- believe that a disaster is unlikely to happen, and are content to accept the risk.
- are busy with other things and continuity planning has a low priority;
- believe that everyone will rise to the ocassion and they will be able to 'muddle through' if a disaster happens;
- are unaware of the business risks, while their users' views are unknown or ignored.
- Continuity planning is often given a "nice to have, but not essential" status in the system development/procurement process, or is overlooked altogether.

1.4 This module

This module describes the process involved in drawing up a business continuity plan and in maintaining it. The final section contains a list of questions that the auditor will need to consider when reviewing a continuity planning project, or the adequacy of continuity planning in an operational It environment.

The reader should now turn to the case studies at Annex 1. These illustrate the sorts of problems that can arise when business continuity planning is neglected, and will help to place the remainder of this module in context. A proforma continuity plan is attached at Annex 2.

2. An approach to business continuity planning

2.1 Contingency and continuity planning

A well designed computer system is usually reliable but, like everything else, it is subject to unpredictable events. When these occur users are faced with a situation where what they believed to be trustworthy has become unusable. Nevertheless they must be able to continue the business during the period of unavailability. As the case studies (Annex 1) illustrate, this can extend for several weeks or, in extreme cases, to months.

Contingency planning has traditionally been the province of the IT Department. It covers the computer room against threats such as fire and flood. But this is not enough to ensure *business continuity* which, after all, is the overall goal. As the case studies serve to illustrate, "people problems" must not be overlooked particularly as IT is increasingly being delivered to the user's desktop. If personnel cannot reach the office, and/or cannot be relocated in suitable accommodation and provided with support services (furniture, telephones, fax, mail, etc), information systems come to a halt and with them the business.

The many questions that need to be addressed when drawing up a business continuity plan cannot be resolved by the IT Department alone. The wider problems that relate to people, communications, office accommodation, vital paper documents, etc must also be resolved. Whereas a contingency plan focuses on specifics, such as the actions that are necessary to transfer a business system to a standby site, a business continuity plan contains everything that is necessary to provide an organisation with the ability to fulfil its corporate mission during the period of disruption, and then to return to normal in a controlled manner.

2.2 The continuity planning process

A range of skills. will be required to draw up comprehensive plans, and because of the large number of questions that will need to be resolved during the planning process, a methodical approach to the task (such as that at Appendix 2) will help to ensure that nothing important is left out. It will also be easier to control the development process if it is initiated and managed as a "project" (see the project management section in the module on IT methods). This will involve :-

- defining the project objectives and deliverables;
- agreeing a project budget and deadline;
- allocating sufficient skills and resources;
- appointing a Project Board to 'own' the project, monitor progress and take any major decisions that are necessary. Management commitment during development might be maintained by inviting a senior manager to chair the Project Board;

- appointing a Project Manager to plan and manage day-to-day activities.

The business continuity planning process can be broken down into a number of discrete stages. A project or steering committee should be appointed to take overall control and to review progress against objectives at the end of each stage. Stages are as follows:

- Preliminary work : this stage involves raising top management awareness, and gaining approval to undertake a scoping survey (probably unnecessary for a small organisation). The survey provides information on which to estimate the costs and timescale, the skills, and the manpower required to undertake a business impact review. A corporate policy on business continuity planning is produced to underpin subsequent development work (this may require refinement as the project progresses). This should cover:
  - on-going management;
  - development of continuity plans;
  - on-going programme of testing;
  - maintenance;
  - arrangements with suppliers;
  - education and training of staff;
  - retention and management of critical information (both documents and media).
- Business impact review : this is a detailed review that builds on the survey. It examines each business system to identify the business impacts should the system cease to function, and hence its criticality to the business. In organisations that carry out bespoke software development, the system development environment should also be included. The review should also identify any obvious areas where controls might be improved in order to reduce risks of disaster.
- Recovery options review : identifies and costs feasible recovery options for each system that is to be covered by the plan. Basic disaster prevention measures are also reviewed in more detail (opportunities were identified during the previous stage), and costed recommendations for enhancements made. Recommendations are made to management.
- Development : during this stage detailed business continuity plans are developed; support contracts and insurance cover, if appropriate, are negotiated; and risk reduction measures are installed. A management framework for maintaining and periodically testing the plan is put in place.
- Awareness and testing : it is very important to raise awareness of business risks, of the corporate continuity policy and plan, and of employees' roles and responsibilities. Personnel must know who to contact in an emergency, where to go, and what is expected of them. The continuity plan must be tested to prove it works.

- Review and update : the results of testing must be reviewed and any changes made (there are bound to be some!). The development project is closed and the continuity plan is handed over to the manager appointed to act as Continuity Planning Manager.

The remainder of this module covers each of these stages in more detail.

3. Preliminary work

3.1 Top management commitment

The development of a workable continuity plan will require a wide range of skills, perhaps involving consultancy support, significant resources, and the co-operation of many personnel in different areas of the organisation. The developed plan will also require an annual budget to cover the cost of awareness training, testing, and maintenance. It is therefore unlikely that any worthwhile progress on continuity planning will be possible without the firm commitment of the organisation's top management.

In order to gain the necessary commitment, and approval to carry out a survey to scope problem, it will probably be necessary to raise top management's awareness of the importance of continuity planning (if that this has not already been raised by a recent disaster!). This can best be achieved by a presentation based on the disaster experiences of comparable organisations together with some initial thoughts on what risks face the organisation in question, and what the potential business consequences might be if they are not properly managed.

3.2 The survey

The objective of the survey is to gather information to support project planning and it should cover all areas of business activity. If the survey is not comprehensive there will be a risk that the an important business process, or perhaps one which produces outputs on which other important processes depend (e.g. data preparation or output distribution) will be omitted from the subsequent business impact review and, in turn, from the continuity plan.

The survey therefore aims to:

- identify all key business systems, their locations, System Owners, users and the business functions they perform; then.....
- identify key business systems or areas that are to be protected by the continuity plan (it will be neither economically feasible, nor indeed necessary, for the continuity plan to cover everything) and which will be included within the business impact review boundary;
- identify technical support staff and others who will need to be interviewed during the business impact review (e.g. Security Manager, Building Services Manager, Trade Union and Staff Welfare officials);
- plan the programme of work to be undertaken during the business impact review, and identify any additional skills that the review team do not have, and which might need to be bought in;

- provide an estimate of costs and time-scale for the business impact review and submit this for management approval.

During the survey system documentation will need to be inspected in order to identify all of the organisation's business systems, and the support services and technical infrastructure on which each depends. A good configuration management database will be of considerable help in identifying computer systems and their technical dependencies.

In organisations that carry out a significant amount of in-house system development it might also be necessary to include the system development in the business impact review. Should important system development projects be brought to a halt by a disaster, there could be serious repercussions on the organisation's ability to meet contractual/political deadlines and to pursue its business strategy successfully.

The survey results in a short management report which identifies the systems to be covered during the business impact review, the skills and manpower resources required to undertake the work, and the review budget and time-scale. The survey will also produce draft terms of reference for the business impact review, and seek management approval.

4. The business impact review

4.1 Objectives

Business continuity must be provided within a reasonable budget. This should take account of both one-off costs, and also on-going costs which can be considerable. If an organisation did not have to worry about cost it could duplicate its entire IT operations. This is an extremely expensive option; nevertheless it is used to protect certain mission critical systems. In all other situations a decision has to be made on which systems must be recovered, and within what time-frame, and which can be ignored for planning purposes due to their lower criticality. The tighter the recovery time-frame, the greater the cost of recovering the service is likely to be.

The objectives of the business impact review are therefore to identify the organisation's business systems and rank them in an order of importance to the business. With this knowledge management are better placed to make an informed decision on how to invest their limited resources.

4.2 Business impact review

4.2.1 Business impact scenarios

System users and IT support personnel will need to be interviewed during the business impact review in order to assess the criticality of each business system within the review's boundary, and to identify the range of threats (and their probability) that might prevent their correct operation.

Identifying potential business impacts will involve considering various "business impact scenarios" (in circumstances where business processes are closely integrated or are highly dependent on each other, and the potential impacts from disruption are similar, the related processes should be considered together). For example, business impact scenarios for a government organisation that administers social security benefits might include the following :-

- state pensions and social security benefit claims cannot be processed;
- benefit payments cannot be made;
- loans cannot be recovered;
- accounts cannot be produced;
- planning statistics cannot be processed;
- personnel cannot be paid;
- voice and e-mail communications cannot be exchanged;
- suppliers bills cannot be paid.

Identifying impact scenarios will involve distinguishing between what is realistic and what is not. This will require a combination of sound judgement and a good all round understanding of the business. A good knowledge of the organisation's history of breakdowns and of the disasters that have affected comparable organisations (together with the type of protection that they have put in place) will help.

4.2.2 Measuring business impacts

Having identified realistic impact scenarios, the related "business impacts" are then measured (ere again records of previous breakdowns will prove useful; for example, how the cost of overtime working increased, or the cost of repairs, etc). Business impacts are estimates of the potential damage to the business that would be caused by an impact scenario taking place. They are estimated for each business process, or group of processes, and it is important to recognise that they will vary with time. In general the longer a scenario continues, the more severe its impact on the business will be. For each scenario it is therefore essential to know the period of time that would elapse before the impact becomes (a) "inconvenient"; (b) "serious"; and (c) "disastrous". Is it minutes? hours? days? etc.

Measures of business impacts fall into two broad categories. "Hard" impacts are those that can be expressed in terms of money (and for this reason can provide a financial justification for investment in business continuity measures).

Hard impacts comprise

- financial loss : for example, the cost of replacing an asset that is destroyed, or the cost of repairing it;
- reduced revenue : arises from an inability to make sales, to control debtors, or the cost of increased borrowing to replace lost or delayed revenue;
- increased cost of working : arises from the need for more overtime working, hiring additional personnel or equipment, or renting additional accommodation;
- financial penalties : arise from breach of contract, failure to meet agreed service level targets, or statutory fines (e.g. failure to pay taxes on time).

"Soft" impacts are those that cannot be expressed in monetary terms reliably.

Soft impacts include :-

- loss of goodwill;
- loss of credibility;
- political, corporate or personal embarrassment;
- breach of the law;
- risk to personal safety;
- loss of operational capability, for example in a 'command and control' environment.

4.2.3 Defining recovery deadlines

Having identified what could go wrong (the "business impact scenario"), how it could affect the business (the "business impact"), and the time that would elapse before this affect took place, it is now possible to rank each process in its order of "criticality" to the organisation. Criticality is expressed in terms of the maximum loss of availability that the organisation can tolerate (on-line systems tend to be less tolerant of disruptions than batch). Systems are ranked in their order of criticality, or if there are many, are placed within categories; for example:

- category 1 : must be recovered within 'n' minutes;
- category 2 : must be recovered within 'n' hours;
- category 3 : must be recovered within 'n' days;
- category 4 : must be recovered within 'n' weeks;
- category 5 : criticality varies according to date (e.g. payroll, payments to suppliers - see case study number 3, Annex 1);
- category 6 : applications that are not critical.

4.3 Risk reduction measures

During the review, the team should identify any areas in which risk of disaster could be reduced by the application of additional controls. However, because the review is not intended to be a detailed review of IT security, this aspect should be confined to more obvious disaster prevention controls, such as those applicable to hardware maintenance and repair; fire and flood prevention and detection; physical access controls; and virus detection. A review of previous security incidents, perhaps based on Help Desk records, will assist in identifying broad areas of weakness.

4.4 Reporting to management

The management report from the business impact review will summarise how much the organisation stand to lose from a disaster or other incident, and how quickly these losses would mount up. The report will therefore identify the key business processes (those on which the organisation most depend), ranked in their order of criticality to the business, and for each one describe:

- the form that the damage or loss to the organisation is likely to take (e.g. lost revenue, loss of goodwill, bad publicity, additional costs);
- how the degree of damage or loss is likely to escalate after the incident;
- the minimum staffing, facilities and services that will be necessary to resume an emergency level of service (i.e. specified priority items only);
- the maximum tolerable time for both emergency and full service recovery.

The Project Board will need to agree the identification and ranking of key business systems, and the estimate of losses that could follow a serious incident or disaster, as these will provide justification for the both the corporate policy and for the project to continue to the next stage, which is to examine and cost specific recovery options, and define a recovery strategy(s).

5. Recovery strategy definition

5.1 Disaster prevention

5.1.1 The basics of disaster prevention

During the recovery strategy stage of planning, the review team should identify any threats that could readily be reduced by the implementation of stronger preventive and detective controls. Stronger controls will reduce the overall risk of a disaster occurring, and will help to prevent serious damage should it occur by ensuring early detection and management. Where insurance (covered in the next section) forms part of the recovery strategy, the insurance company will probably wish to satisfy themselves that there are adequate disaster preventions controls in place, and may require the organisation to make further improvements before they are prepared to accept the risk.

A full assessment of IT security risks and controls is outside of the scope of a business continuity planning project. However the basics of disaster prevention are fairly standard, and the following controls should be considered :-

- site and building access controls, and intruder detection systems;
- fire detection and suppression equipment;
- 'no smoking' and control of inflammable material (e.g. waste, fuel and cleaning fluid) to reduce the risk of fire;
- securing vital non-magnetic records (papers, microfiche, microfilms);
- procedures for dealing with personnel who are dismissed for any reason;
- avoidance of key staff (i.e. individuals who have unique and essential skills);
- arrangements for maintaining equipment in a good state of repair;
- an on-going security awareness campaign;
- backup, storage and recovery of computer systems and data.

5.2 Backup, recovery and media storage

5.2.1 Backing up

"Backing up" is about saving data, programs and system files from a computer system to enable the recovery of lost data, or to handle the complete loss of the system.

The key feature of any business continuity plan is the backup strategy. If backup copies do not exist, cannot be accessed or cannot be restored, then no amount of continuity planning will replace them.

The recovery options stage of continuity planning project should review the adequacy of the organisation's backing up strategies, together with the arrangements for storing backup media and for testing system recovery periodically.

Every system will need at least two copies of its main operating system and major application packages. One copy should be held on site as the immediate recovery copy; another should be held in the remote media store so that in the event of the computer room being destroyed the system can be restored at a standby site. New backups should be taken whenever amendments are made to the operating system or to applications.

Both transaction and master files must be backed up at a frequency that will enable data to be restored whenever the original copy becomes unusable or unavailable for use. If backup copies are seriously out of date they may be of very little value. System configuration files will also need to be backup up but as these are usually less volatile than data they will not need to be backed up as frequently.

5.2.2 Backing up techniques

Backup files must be stored on a separate disk or tape from the original files otherwise they will be as vulnerable as the originals. A record must be kept of the contents of each backup disk or tape, and of its storage location. The main backup techniques are *full copy, file copy and record copy*.

5.2.3 Full copy

The simplest method of backing up a system is to copy the entire contents of its disks/tapes to other disks/tapes. It is a comparatively simple process to carry out and provides a copy of everything. However it suffers the disadvantages that it requires the most time and backup media to complete - and also the most time to restore - and is likely to contain many files that haven't changed since the previous backup. Nevertheless a full backup should be taken periodically to provide a baseline to which more selective backups can then be applied.

5.2.4 File copy

Here only particular files are backed up. These might be files that have changed since the last full copy, or files that relate to each application can be backed up separately so that each application can be readily transferred to another machine in an emergency. The advantages of file copy are that less backup media is used, so it is quicker and cheaper to complete and individual files can be saved and restored as necessary. It suffers the disadvantages that the user must set up a regular routine of saving specific files before or after updating, and the machine still needs a full copy periodically.

5.2.5 Record by record

When using database or on-line systems, where individual records are over-written, it is vital to retain a previously correct version of each record to be updated by copying it to a backup file before it is updated. This protects against errors during updating and provides access to previous versions. The advantages of this approach is that storage costs are minimised and it provides an audit trail by making it possible to review changes to data from a previous date. The disadvantages are that it is difficult to restore records because the appropriate record must be found, erased from the live file and replaced by the last backup copy. A full copy of the database must also be taken periodically.

5.2.6 System recovery

Recovery procedures must be tested periodically to prove that all the components that are necessary to restore the system are in fact being backed up correctly. If recovery does not work the backup copies will probably be useless.

Tests should be practised in conditions that resemble as close as possible a real emergency when the system may have to be restored within a tight timescale and in unfamiliar surroundings.

5.2.7 Media storage

A record should be kept of all backups taken so that there is no doubt as to the copy which should be used. Although a strict schedule of documented backups will make recovery possible, **it is only a part of the equation**. Good media storage facilities, together with a workable recovery process, are also among the essential components of a business continuity plan.

Backup copies should not be stored in document safes. Purpose-built magnetic media safes are capable of protecting magnetic media against the temperatures found in a burning building, and are also waterproof. Because of the additional protection they have to provide, magnetic media safes are much heavier than document safes. The safes must not be left open because in an emergency there is unlikely to be sufficient time to lock them.

Some of the backup copies should be kept at a remote site that is well removed from the major cause that is likely to destroy the originals. If there is a fire or bomb blast, and access to the home site is denied, the remote copies will be available before those

in the fireproof safe. A further benefit of remote storage is that it also affords some protection against malicious staff at the home site.

5.3 Non-technical options

In practice a recovery strategy is likely to be a mix of technical and non-technical recovery options. The following are examples

5.3.1 The "do nothing" option

In this age of increasing reliance on computer systems the 'do nothing' option is increasingly difficult to justify except for low risk systems, or those that can be quickly and easily replaced quickly "off-the-shelf". This approach is more likely to be based on the mistaken belief that a disaster will never occur.

The 'do nothing' option does not of course apply to the need to back up data, and for remote storage.

5.3.2 Clerical backup procedures

This option involves falling back on clerical procedures. However, when an organisation computerises its business processes, its personnel quickly lose the skill required to perform the task clerically, while the user manuals and stationery that is necessary to support clerical processing is discarded. Computerisation also results in reduced numbers, so regardless of a skills shortage there may be insufficient personnel to maintain an adequate level of service.

Clerical backup procedures are therefore only feasible for small systems, or as a temporary measure in the period immediately following a disaster when a limited service needs to be provided until standby computer processing becomes operational (e.g. in issuing payments to personnel and suppliers). Where clerical procedures are used, the continuity planners must ensure that there is an adequate supply of stationery, and also written procedures, in the remote media store and/or the Emergency Control Centre.

5.3.3 Insuring the risk

Insurance policies provide a way of recovering capital costs after a disaster. The insurance company will usually inspect the premises and might require standards to be improved since the likelihood of loss to them, by way of settling a claim, is increased if the design of the building, or parts of it such as the computer room, is dangerous, or if fire precautions are neglected. Bespoke insurance to match individual organisations' exact needs can be obtained from specialist insurance brokers. The risks to a computer centre that can be insured against can be categorised as:

- **material damage** : applies to risks involving replacement or repair of equipment as a direct cost. Cover can be obtained for computers, communications and environmental equipment against most risks, possibly including malicious damage, but excluding wear and tare, and electrical and mechanical breakdown;
- **consequential loss** : loss due to a company's continuing inability to maintain its computer service as well as the increased cost of emergency working and the cost of restoring the service. Premiums may be substantial if they are to cover the total period of unavailability;
- **risks to and from staff** : includes injury to staff, and damage caused by disgruntled or bored staff.

5.3.4 Leasing equipment

Rental or leasing agreements will provide cover for the replacement of hardware, but consequential losses will be excluded and must be insured separately.

5.3.5 Outsourcing the service

"Outsourcing" can be an effective way of strengthening system resilience by giving the bulk of the continuity planning problem to another organisation who are better equipped to do the job.

Outsourcing takes place when an organisation contract with a specialist "IT service provider" for the provision of a complete IT service. The service provider owns the hardware and software, and provides the accommodation and the personnel to operate and maintain the system. But outsourcing has much wider implications than just continuity planning. It is an approach to business management that permits an organisation - for whom IT is a subsidiary activity - to focus on its core business, and to achieve savings through the economies of scale that can be obtained by a specialist "IT service provider".

A further advantage of outsourcing is that the IT service provider becomes responsible for delivering a specified level of service to the customer organisation. For example, the service contract may require the delivery of an on-line accounting system to the organisation with, say, no greater service break than 30 minutes and not more than 1 hour total downtime in any rolling 4 week period. In order to achieve the specified service level, the service provider will need to develop an appropriate business

continuity plan to cover service failures and disaster. As the service provider's computer installation is generally shared by a number of customers, the overall cost of providing and maintaining the continuity plan will be shared between them. It is also likely that the service provider can afford to provide more sophisticated continuity arrangements than any one customer.

Thus outsourcing can represent a recovery option, particularly for small organisations who can not afford the cost of developing and maintaining their own continuity plan. However, it must not be forgotten that after taking account of what has been outsourced, some business processes will inevitably remain that will need to be considered for continuity planning.

5.4 Technical options for recovery

The business impact review identified the business systems that need to be covered by the continuity plan, and their priority for recovery. During this stage the range of technical options for recovering each system is examined and costed. The types of technical options considered will depend on the nature of the system in question (e.g. batch, on-line, PC-based, mainframe) and the time-frame within which it must be restored to service. Generally speaking the shorter the recovery time-frame, the more expensive the recovery arrangements are likely to be.

Technical options for recovery fall under the following headings.

5.4.1 Mirrored systems

Mirrored systems are a comparatively high cost option that are nevertheless justified for mission critical systems, where even a small loss of availability would have a severe impact on the business (e.g. airline reservations; treasury systems; some banking operations). This approach involves running two (or more) systems at different locations, possibly many miles apart, and updating each in parallel. One system carries the live workload but it is possible to switch to the mirrored system without noticeable disruption of service should the need arise.

5.4.2 Hot start

This is a fully equipped processing facility that is ready to operate within hours. In order to use a hot start site its equipment and system software must be compatible with the installation being backed up, and it must offer sufficient storage capacity and processing power. The only additional needs are programs, data files, documentation and personnel, and support services (e.g. telephones, fax, mail, etc) if these are not already provided.

5.4.3 Warm start

This is a facility that is partially equipped (with environment, communications connections, storage devices and controllers) but without the main computer, the assumption being that this will be readily obtainable. As the computer is the most

expensive component, the warm start is cheaper than the hot start option but will take several days to bring into operation.

5.4.4 Cold start

A facility that offers only the basic environment (electrical wiring, air conditioning, flooring, etc), but is ready to receive equipment. Cold start might take several weeks to activate.

Disaster recovery contractors generally offer “hot” and “cold” facilities as either fixed or mobile (i.e. on the back of a truck) options.

5.4.5 Reciprocal agreements

These are agreements between two or more organisations, with similar equipment and business systems, to provide each other with standby computing facilities in an emergency. Although reciprocal agreements are a low cost option, they are not usually legally enforceable. They also depend on the various parties to the agreement continuing to maintain spare capacity and compatible systems and are therefore more appropriate to different sites within the same organisation, where a common IT strategy is being followed.

If a reciprocal agreement is implemented between different organisations, it should be supported by:

- a signed written agreement specifying the type and level of service to be provided, for how long, and under what circumstances;
- a change management system that will help to ensure adequate capacity and system compatibility.

5.4.6 Fortress approach

The philosophy underlying the fortress approach is to remove the risk, or reduce it to insignificant proportions. Its advantage is that it dispenses with the need to move to a standby site with all the costs and logistical problems that that entails. Instead money is spent in making the home site as disaster-proof as possible, with lots of built-in redundancy together with high quality environmental, physical and logical controls. However, it must be recognised that it is impossible to protect a site from all possible disasters.

5.5 Reporting to management

The recovery strategy review should result in a report to management which describes the continuity options that appear to be feasible for each business system (or category), estimated one-off and on-going cost implications of each, and a recommended course of action. A further important output from the strategy review is to recommend a corporate policy on business continuity. This will be based on the

recovery strategy, and will recommend to management what the organisation's business continuity objectives ought to be.

It will also be necessary to prepare an estimate of the personnel, skills and funding required for the next stage of development, which is to produce a detailed business continuity plan.

The detailed continuity plan that is developed during the next stage of the project will implement the corporate continuity policy and also under-pin the continuity awareness training programme.

6. Developing the business continuity plan

6.1 Levels of business disruption

If a business impact review has been carried out thoroughly, the review team will have gained a clear overview of the organisation's key business systems and how they interact. The business impact of their unavailability will determine which systems are to be recovered, their order of recovery, and the time-scales involved which in turn will determine the backing up strategy and the most suitable method for system recovery (hot start, cold start, etc.).

The completed Business Continuity Plan must contain all the information needed to recover the business following a disaster. However, what constitutes a "disaster" will depend on an organisation's ability to absorb damage, and this will relate to its economic strength. The business consequence of a disaster will also differ between the private sector, where 'going out of business' is a real risk, and the public sector where the major impact could well be the extent of the political embarrassment suffered by the government and senior civil servants. The following is therefore only a guide to the sorts of factors that might distinguish between minor and major problems, and a disaster.

- Inconvenient : a disruption to the business process stemming from a minor failure of a key business system, or its supporting services. System users are not expected to suffer more than a minor reduction in service, and it is expected that the organisation will continue to be able to meet their contractual and legal obligations throughout the disruption. Computer systems need to be recovered from backup and/or minor repairs made. Limited overtime working and/or extra staff are necessary to investigate the problem and to achieve full recovery. *It should not be necessary to activate any part of the business continuity plan.*
- Serious : a failure of one or more key business processes stemming from serious damage to corporate data and/or equipment, but not serious damage to buildings. Alternatively the incident may result from a severe failure in the utility supply (e.g. telecommunications, electricity, water supply). The incident results in a severely reduced level of service to customers, which may be restricted to high priority items, and a loss of goodwill. The organisation run a high risk that they will be unable to meet their contractual and legal obligations, unless they take prompt emergency action. Overtime working and/or additional personnel are needed to implement emergency working, diagnose the problem and make repairs, recover services, and clear the backlog of work. The incident (or its cause) attracts limited comment in the media. *It will be necessary to activate parts of the continuity plan in order to assess the damage, provide standby processing and an emergency service to customers, and eventually to resume normal working.*
- Disaster : failure of a number of key business processes stemming from serious damage to corporate data, equipment and buildings. The incident may also

cover a wide locality (e.g. severe weather conditions) and involve severe failures within other organisations that supply essential goods and services (e.g. utility supplies). There is a complete break in services to customers, and a significant loss of goodwill. The organisation will be unable to meet their contractual and legal obligations unless they take prompt emergency action. Both computer processing and system users need to be re-located. Extensive repairs are necessary at the home site and emergency working is likely to continue for a significant period. The incident attracts widespread comment in the media and is likely to be discussed in the legislative assembly. *The full business continuity plan, including both short and long term strategies, will need to be activated.*

6.2 Sections of a continuity plan

The contents of a business continuity plan will vary according to circumstances, but in general it will need to contain detailed information under the following headings.

6.2.1 Administration

This section will contain information on how and when to invoke the plan; the programmes of action to be entered into; the personnel involved; and where the Emergency Control Centre is located. The plan will also need to identify the personnel who are authorised to invoke particular sections of the plan, or the entire plan.

Following a serious incident, the Crisis Management Team will need to decide on the most appropriate course of action to take. This will largely depend on the length of time the disaster is expected to last, the criticality of the business systems that are affected, the amount of damage sustained, and the amount of damage the organisation are likely to sustain if prompt action is not taken. They will need to organise their recovery teams quickly and arrange for an initial assessment of the situation to be made. This will provide information on which to assess the length of time that the outage is likely to continue, and will help to determine the most appropriate course of action.

Separate categories of continuity plan may be needed to cover different levels of damage and business disruption. For example :-

category	**anticipated outage**	**damage/disruption**
Inconvenient	3 days	limited
Serious	3 < 7 days	serious
Disaster	>= 7 days	severe

Effective disaster recovery will depend on quick and effective use of key personnel. This can best be achieved by organising a number of recovery teams to take over areas of responsibility and undertake specific tasks. The following are some examples of how personnel involved with emergency response and recovery might be deployed.

Crisis Management Team : a small team comprising managers representing personnel, IT, building services, finance and under the direction of the Continuity Planning Manager. Their role is take control of disaster recovery; invoke the continuity plan; liaise with top management; manage and co-ordinate emergency operations; and plan and manage the return to normal working;

Security Team : maintain security at the home site and implement security at the standby site as required. Organise and assist with salvage of media and vital documents from damaged premises;

Building Services : assess damage and plan for repairs. Liaise with utility suppliers (gas, water, electricity, etc) on re-connection of supplies. Implement support services at standby site (e.g. office equipment, mail, telephones, fax, stationery, etc);

Computer Operations Team : liaison with maintenance engineers. Supervise supply and installation of replacement equipment. Liaise with users on service recovery. Recover backup media from remote storage. Re-establish backing up procedures and a new remote store for the standby site. Recover computer processing commensurate with business priorities;

Telecommunications Team : liaison with telecommunications and network suppliers on re-connection/transfer of data communications facilities at home/standby sites.

6.2.2 Support contracts

Details of any contracts and agreements (including software licenses) that have been entered into to support business recovery and the re-ordering of equipment and services.

6.2.3 Computer operations

The instructions which, together with the following sections, are necessary to enable the key computer processes to be recovered following an emergency, including any relaxation of service levels that might apply.

6.2.4 IT Infrastructure

Detailed lists of the hardware, telecommunications and software that comprises the replacement system(s). Lists of companies to be contacted to supply services or equipment needed for recovery, and the procedures to be followed for ordering replacement equipment and/or services. A current version of the IT asset register should be included with the documents stored in the remote store to assist with the re-order of hardware and proprietary software.

6.2.5 Remote media store

Identifies the location of the remote media store, lists of the items that are stored there, and arrangements for gaining access. Also describes the location of the remote media store for the standby site, if this is different, and the backing up procedures to be followed during emergency operation.

6.2.6 Personnel

Identifies the personnel who will need to be re-located at the standby site. Details of personnel welfare and trade union arrangements. Identifies sources of additional personnel (e.g. from elsewhere in the firm; contractors; consultants; bureau/agencies).

6.2.7 Home site

Contains instructions on how security and salvage at the home site is to be provided if the site is extensively damaged and needs to be evacuated.

6.2.8 Standby site

Identifies the :-

- people to be contacted at the standby site in the event of an emergency;
- transport arrangements;
- accommodation that will be available and the uses for which it is suitable;
- existing security arrangements and details of any changes that will be needed;
- living accommodation available for personnel who will be unable to return home.

6.2.9 Return to normal

Contains a detailed list of responsibilities of the various teams involved in repair and rehabilitation of the home site. After an eventual return to normal the Contingency

Planning Manager should assess the effectiveness of the plan and instigate any changes that are necessary.

6.3 Supporting requirements

The business continuity plan must not focus entirely on IT requirements. People are an essential requirement because there is no point in recovering a business system that cannot be used. Other needs on which successful business recovery will depend are as follows.

6.3.1 Evacuation

Personnel are the most important corporate asset. The organisation cannot function without its personnel no matter how much equipment and data are available to it. The key aspect of the recovery plan must be to ensure that personnel are safely evacuated from any business area that is threatened. Building services and external agencies such as the police and fire services will need to be consulted on the provision of emergency exits, internal voice communications, emergency lighting, and evacuation areas.

6.3.2 Emergency Control Centre

Taking control of a disaster at an early stage will help to minimise the general confusion that is bound to follow a disaster, restrict the spread of damage (e.g. protecting the contents a damaged building from intruders and the weather), and enable the prompt recovery of key business systems.

An Emergency Control Centre provides a location at which the Crisis Management Team can be based. It will need good communications facilities to enable links to be maintained with the disaster recovery teams, other parts of the organisation, outside contractors and agencies, personnel and top management. It will also need to be equipped with meeting rooms and perhaps limited sleeping accommodation.. As the World Trade Centre case study illustrates, the emergency control centre must be located well away from the potential disaster area.

6.3.3 Vital records

Much information that is essential to the effective conduct of business may exist on paper. For example, important correspondence; contracts and other legal documents; information stored on fiche and microfilm, and source documents that support data held on computer.

Other documents that are often essential to disaster recovery include :-

- the business continuity plan;
- contracts with disaster recovery companies, and insurance policies;
- home addresses and telephone numbers of personnel;
- addresses and telephone numbers of equipment suppliers and support services;
- equipment lists;
- user and operational manuals;
- procedures for running operations manually in an emergency, together with a good supply of stationery;
- a supply of cheques for paying employees and suppliers.

Although it may be the ideal solution, it is not always possible to ensure that copies of all vital records - either as paper, microfilm document image - are held in a remote store due to the large volumes that are involved. If vital records cannot be backed up in this way, they should at least be stored in appropriate fire-proof containers at known locations so that they may be recovered during a salvage operation. A summary of what vital documents are held (in particular contracts), and where, should be kept at the Emergency Control Centre.

6.3.4 Re-locating personnel

Personnel might have to be re-located at sites that are a considerable distance from their home base. Not only will this involve the cost of transport and hotel accommodation, but there is also the disruption to private lives to consider. Planning for re-location will involve identifying surplus accommodation within the organisation, but away from the home site; leasing additional capacity; or contracting with a supplier of mobile office accommodation.

Perhaps an important assumption that might weaken the plan is that personnel - particularly key personnel - can get to the office. This might not be the case following a large scale natural disaster when many may have been left homeless or are unable to reach their place of work (e.g the aftermath of hurricane Andrew in Florida). This aspect of continuity planning will need to examine ways in which the organisation may first have to provide welfare assistance to their work-force before they can expect them to be in a position to return to work. This will involve input from the organisation’s staff welfare and trade union groups. The possibility of transferring work to other parts of the organisation, shipping personnel out, or bringing personnel

in will need to be examined, and in the face of a shortage in airline reservations (e.g. case study number 2, Annex 1).

6.3.5 Re-establishing support services

Most modern computer systems are on-line; they are operated by the users from the desktop and therefore require office accommodation. To be of any use emergency accommodation must be provided with appropriate support services. These will include heating, lighting and air-conditioning; office furniture; PCs/terminals/printers; postal services; and building security. Perhaps the most difficult service to recover, particularly after a large scale natural disaster (hurricane, flooding, severe snowfalls, etc) will be communications with the outside world.

6.3.6 Salvage

Certain types of disasters (e.g. bomb blasts, fires and earthquakes) might leave the home building badly damaged and important and potentially sensitive documentary records unprotected from the weather, or quite literally blowing around the neighbourhood, and some of these records may be essential for business recovery purposes. The plan's developers will need to consider how salvage operations - possibly involving entering a dangerous building - will be conducted and by whom. Additional security guards might be necessary to prevent looting.

An aspect of salvage that may need careful attention is the disposal of damaged magnetic media. People are generally aware of the need to safeguard paper files, but that does not always apply to magnetic media which might contain information that is either sensitive in the context of national security or is commercially sensitive. Although the media may be beyond economic recovery, it is possible to recover the data in some circumstances even if the media is badly damaged. It will therefore be necessary to ensure that an adequate level of security applies where magnetic files, or devices that contain magnetic files (e.g. personal computers) are removed from site for repair or disposal, and this might involve ensuring that all damaged magnetic files are destroyed, either by burning or fragmentation (effectively grinding them up).

7. Training, testing and updating

7.1 Training

A business continuity plan will have very limited value if personnel are unaware of its requirements, such as the role that they are to play in an emergency. As development nears completion, the project team will need to provide key personnel with training in the role that they are to play in an emergency; and this will at any rate be necessary to enable the plan to be tested. Those who do not have a specific role in the plan will also need to be made aware of the basics, such as, why a continuity plan is necessary, who will be in charge, where they are to go, who to contact, etc.

The training programme must aim to ensure that all those that are to be involved in activating and managing the plan are aware of their role and responsibilities, and have the appropriate skills to carry them out. This might involve specialist training in emergency and recovery procedures. To help avoid any misunderstandings or failure to recognise the importance of the business continuity, the job descriptions and/or contracts of employment of members of the Crisis Management Team, the disaster recovery teams, and any other key personnel should include a clear definition of their particular roles and responsibilities in relation to the plan.

All other personnel must be made "aware". Awareness training will not simply be a matter of providing everyone with a copy of the business continuity plan. The completed plan will probably be a fairly large and technical document, and it is unlikely that the uninformed reader would gain much information on the overall need for a plan, or in their particular role. The plan might contain sensitive information that is not for a general distribution.

Awareness training is best kept short and simple, and directed at small groups of personnel who work with the same business system, or in the same business area, and who are likely to share common problems during an emergency. Although well designed leaflets and posters provide useful reminders they should not be relied on as the primary source of training because they are not widely read, or their importance recognised. Awareness training should instead be based on presentations given by members of the project team, and these might be supplemented by video material to illustrate the sorts of disasters that can occur. There is no shortage of commercially available training videos on disaster prevention and recovery.

In the longer term awareness training 'reminders' will need to be given, particularly where there has been a change in the continuity plan (e.g. following the introduction of a new business system) or to ensure that everyone knows the part they are to play before the plan is tested. Awareness training, probably on security as a whole (keeping passwords secret; computer virus policy; locking sensitive papers away; fire prevention, etc) should be included in the induction course for new recruits.

Finally, where a standby site and emergency office accommodation is involved, arranging for groups of staff to make a guided tour of the premises where they would be required to work in an emergency will make an effective contribution to their awareness training.

7.2 Testing the plan

The completed business continuity plan not only represents a valuable form of insurance for the business, it also represents a considerable investment in cost and effort. To retain its value, the plan must be kept up-to-date. This will involve changing it from time to time to keep pace with changes in business objectives and in the surrounding business environment (e.g. new or modified computer systems; parts of the business transferred to new locations; different threats; different business system priorities), and then testing the plan to gain assurance that it meets business needs and remains workable.

The overall objectives of testing are to ensure that :-

- personnel are aware of their roles and responsibilities;
- personnel are able to perform their roles;
- changes that are necessary to ensure that the plan remains both workable and up-to-date are made.

Full testing should take place before the plan is accepted and further testing carried out regularly thereafter. The plan should also be tested when any major system changes result in a significant revision of the plan. There are various approaches to testing.

Live testing : should be carried out under conditions that are as realistic as possible (case study number 6, Annex 1). The test should be based on a major disaster scenario and involve transferring the live workload on the key systems under test to a standby system(s). It should also be carried out under the control of the Crisis Management Team at the Emergency Control Centre, and include re-location of some business users in line with the test scenario and the plan's requirements.

Overall the test should aim to prove that :-

- the system(s) under test can be recovered on the standby computer;
- the correct system and data files are being backed up;
- the standby system remains compatible with the main system;
- telecommunication links (both voice and data) can be switched to the standby site;
- procedures for re-locating personnel in an emergency work;
- user support services can be provided.

This approach to testing the continuity plan is likely to be the most effective providing that it is well planned and managed. It is also likely to be the most expensive strategy and the one that results in the greatest amount of business disruption unless tests are timed to coincide with periods of low business activity. Despite these obvious drawbacks, live testing should be carried out periodically as it is the only means of gaining adequate assurance that the plan does work in practice and is dependable.

In the period between live tests the other intermediate strategies described in the following paragraphs provide an effective supplement to, but not a replacement for, live testing.

System recovery (or restricted live testing) : earlier sections of the notes emphasise the importance of both backing up and being able to recover systems from backup. Recovering systems, particularly on a standby computer, is an exercise that also ought be carried out periodically. Even if the recovered system only carries a simulated workload, the exercise will at least provide assurance that aspects of the plan remain workable. Variations on this type of testing might include :-

- unannounced tests;
- random selection of staff to be involved in the test, reducing the work-force and excluding some key members of the team;
- disabling major system components to simulate failures.

Standby utilities : these mainly include standby supplies for electricity, water (for coolant) and telecommunications. The standby generators and/or uninterrupted power supply should be tested at least monthly under full load. During an emergency, the standby power supply might need to maintain key computer systems, their supporting environmental equipment (humidity control, chillers, ventilation fans, etc), and communication systems (intercom, telephone, radio, fax, data, etc).

Testing that the emergency water supply remains available and sufficient to meet needs should not be over-looked. It is also possible that a failure in the local telephone exchange or in one of their principal links may need to be covered by standby radio circuits or cellular telephone links. These services should be tested periodically.

Practice evacuations : in many countries it will be a legal requirement to carry out one or more practice evacuations of the building each year. Practice evacuations can be used to exercise both the Continuity Planning Manager and the Emergency Control Centre, but are most useful for maintaining personnel awareness.

Dry running : involves taking a board game approach to the problem. An imaginary scenario is created and the team involved talk through their roles in implementing the plan and managing recovery.

7.3 Evaluating the results and updating the plan

7.3.1 Evaluating the results

Testing is not simply a matter of going through the motions. The objective must be to prove that the plan is workable. Testing should therefore be underpinned by criteria that can subsequently be used to evaluate the test results. Test criteria will generally be time-related, and include :-

- **time to restore the system under test**. If this is excessive and business operations cannot be restored within the critical deadline, then either further testing will be necessary to improve familiarity with implementing the plan, or it will need to be modified in some respect(s). This test might include a number of subsidiary timings, such as that taken for the Crisis Management Team to take control; for the disaster recovery contractor to respond; for backup copies of data and software to reach the standby site; for the system to be recovered; for processing to be restored; etc
- **time to reconnect users to the system under test**. Restoring a batch system might pose different problems to those presented by an on-line system where problems might be experienced with diverting telecommunications circuits and restoring LANs (case study number 1, Annex 1);
- **time to distribute printed output**. If printed outputs are produced centrally, can these be distributed to the correct recipients - who may be located in emergency accommodation away from the home site - within an acceptable time-frame? (case study number 6, Annex 1);
- **processing load**. It is possible that the standby system, when recovered, might be unable to process the necessary volume of traffic or offer a satisfactory response time, even taking account of the possibility that a reduced level of service might be acceptable under emergency conditions (case study number 3, Annex 1);

Experience shows that initial testing can go drastically wrong. In these circumstances it may be preferable to abort the test, but if it is allowed to continue, the problem(s) should be recorded for subsequent analysis and action.

A problem log must be kept in which to record all problems that arise during testing. Following the test, problem data should be classified by type and ranked by severity. This information will provide further criteria against which to judge the overall

success of the test. It will also provide indicators for where the plan will need to be changed.

7.3.2 Updating the plan

Perhaps the most important requirement under this heading is to ensure that the plan has a recognised "owner"; that is a manager who is accountable to the Board for the maintenance of a workable continuity plan. Lack of an owner will inevitably result in the plan falling into obsolescence. This "role" (except in the largest organisation it is unlikely to constitute a full time job), perhaps described as Continuity Manager, will probably fall to the organisation's Security Manager due to the relationship of business continuity planning with other aspects of corporate security.

Businesses rarely remain static for long. Their priorities and objectives change, as do ways of meeting them; computer equipment becomes obsolete and is replaced, a change which in turn often leads to changes in working methods (e.g. the move from batch to on-line systems); and organisations and their departments move location periodically. If changes such as these are not accurately reflected in the continuity plan, it will gradually cease to reflect reality. For example, what is the point of having a contingency plan for the mainframe, when the organisation disposed of it when they moved to client-server technology?

The continuity plan must therefore keep pace with changes to key business systems. "Impact assessment" is an important aspect of change management by which change proposals are circulated for comment to all business managers who might in some way be affected by a proposed change. The Continuity Manager should be included on the circulation list for all significant system changes so that he/she can assess the extent to which the plan will need to be altered if a proposed change goes ahead, and bring to bring to the project manager's attention any cost implications.

But the most important way of ensuring that the plan remains workable is to test it periodically, to review the test results, and to update where necessary.

8. Audit considerations

If the organisation do not have a business continuity plan the auditor will need to ascertain whether any of their business systems - both manual and computer - are sufficiently critical to justify the cost of developing and maintaining a continuity plan. If, in the auditor's opinion, the "do nothing" option cannot be fully justified, the matter should be brought to the attention of top management to ensure that they are aware of the extent of their exposure to disaster.

Regardless of the need for a business continuity plan, there ought to be a workable (i.e. has it been tested?) strategy designed to ensure that computer systems can be recovered from backup within an acceptable time-frame. And at least one full copy of the backup should be stored remotely.

Other questions which the auditor will need to consider when reviewing a business continuity plan are as follows.

a) Is the continuity plan documented? *It is very unlikely that an undocumented plan will prove effective either to support testing or in a real emergency*.

b) Does the plan define what will constitute a "disaster" or "emergency", who will take control should one occur, and from where control will be exercised? *A plan will be of very little use if it is unclear who will be responsible for implementing it, under what circumstances, and from where control is to be exercised.*

c) Is the plan based on risk assessment? Has the maximum tolerable outage for each key business system been defined? Has an order of system recovery been specified that reflects the criticality of each system? *It is unlikely that the organisation will be able to afford to protect all their systems, or that this is indeed necessary, so resources must be focused on those systems that are most important to the business.*

d) Does the plan take full account of non-technical needs, such as the re-location of personnel, and the diversion of support services to their emergency accommodation? *There is no point in recovering business systems if their users cannot be connected to them and supported in other ways that are essential to their operation.*

e) Are the disaster recovery strategies for each business system appropriate to its criticality? ('hot start', 'cold start', etc) *An inappropriate recovery strategy will prevent the system from being restored within its critical time-frame.*

f) Has the plan been allocated an adequate financial budget to pay for annual testing and maintenance? *No plan will remain up-to-date, and therefore dependable, for long in the face of changing business needs. Plans must be tested regularly to prove their dependability and updating as necessary.*

g) Has a manager of appropriate status been appointed as Continuity Manager, or have other effective arrangements been made which ensure that the plan has an "owner"? *If the plan does not have a clearly recognised owner it will gradually become obsolete through lack of updating.*

h) Where are copies of the continuity plan held? *To ensure that the plan is readily available in an emergency the minimum distribution should include copies in the remote store, the emergency control centre, and both at the homes of all key personnel involved with its implementation. Other organisation who are closely linked to the plan (e.g. linked by a reciprocal agreement) might also need to have a copy to define the roles that they are to play.*

i) Does the plan contain a version number to indicate the currency of each section, an up-to-date circulation list and a record of the amendments that have been made to it (i.e. have all amendments been incorporated in this copy*?).* Are out-of-date versions of the plan collected and destroyed? *Out-of-date versions of the plan must be easy to recognise because it is unlikely that they will be of much use.*

j) Testing the plan.

- Have the organisation an adequate strategy for testing the plan?
- Does the strategy include the need to carry out complete end-to-end testing under a full live load periodically? Has the plan been tested in line with the strategy?
- Were test criteria set before the test to help measure effectiveness? Were test results analysed against the criteria? *Targets are necessary to ensure that key systems can be recovered within an acceptable time-frame.*
- Was a report to top management produced to summarise test results, the overall conclusion reached, and to specify where changes are necessary?

k) Awareness training.

- Do personnel know what action they are to take in an emergency? (e.g. where to go, who to contact, what to do);
- Are users familiar with the standby site?
- Are building evacuations practised periodically?
- Are personnel included in live tests of the continuity plan?

l) Backup and recovery *(the auditor will need to exercise judgement in deciding whether the backup strategy is adequate. Its nature will depend on the rate of change of data and software, and the criticality of the system to the business).-*

- Has a backup strategy been agreed between user and IT management's? If adequate backup does not exist, many aspects of the continuity plan might become worthless.

- Does the frequency of backing up defined in the strategy adequately reflect the rate of change of the underlying files and the criticality of the system?
- Are a sufficient number of backup copies taken at each pass to allow for distribution of the copies between media library, fire-safe and remote store? Also, to protect against the possibility of a defective tape or disk?
- Does the backup strategy adequately address the need to take full system backups taken periodically?
- Are a sufficient number of generations of backup maintained to allow the system to be rolled back and restored from an dates? *A system error might extend over a number of processing cycles before its effects on system data are detected. This might mean that the system will need to be recovered from its state some days, or possible weeks, previously*
- Is a log maintained of the serial numbers of backup media, their contents and their location? Is a copy of the log maintained at the remote media store?
- Is a full system restore test periodically to prove the integrity of the backup process? Are these repeated on standby computers to prove that the system can be transferred to a standby site?

m) On-site and remote storage.

- Is a purpose-built fire/water proof safe provided for the on-site storage of backup media? Is the safe kept locked when not in use?
- Is a secure store well removed from the home site provided for the storage of backup media and copies of vital documents? *The remote store should be at such a distance that access will not be affected if access to the home site and its immediate neighbourhood is denied.*
- Are physical access and environmental controls at the remote store sufficient to safeguard backup material against threats such as fire, water-damage, unauthorised copying and theft? Is the remote store located near to anything that might endanger its security, such as water tanks and pipes, central heating boilers and heating oil, cooking equipment? *All the latter increase the risk of fire or water damage.*
- Are copies of important paper records held in the remote store? (e.g. user and operations manuals, telephone directories, equipment lists, lists of equipment suppliers and maintainers)
- Is access to the remote store guaranteed at all times? This will include access to the site or building housing the remote store, and to any keys or key combinations that are necessary to unlock cupboards, etc.

n) Emergency Control Centre : has an off-site location been designated for managing an emergency should the home site be damaged or access to it denied? Have adequate facilities in the form of telephones, faxes and meeting rooms been provided? Is an up-to-date copy of the continuity plan and

telephone directories held there? Also an adequate supply of stationery? (including cheques)

o) Vital non-magnetic records : have non-magnetic records (papers, fiche, microfilm) that are vital to the business process been identified? Is their location known? (*to facilitate salvage*) Are they stored in appropriate containers? (*to prevent damage*) To the extent that it is feasible to do so, have duplicates been transferred to the off-site store?

p) Security at the home site : have adequate measures been made for protecting the home site in the event of severe damage to the buildings? (*following fire, storm damage, bomb blast, etc*). Does the plan include procedures for salvaging vital records? (*both magnetic and non-magnetic*) Does the plan include instructions for secure disposal of damaged magnetic media?

9. Appendix 1: case studies

1: Fire - Digital Equipment Corporation

On 6 March 1990 a fire started at the Basingstoke headquarters of DEC UK. The fire rapidly spread through the ceiling void of the building, and although 100 firemen and some 20 appliances were soon in attendance, the roof and upper floor of the building were quickly gutted.

DEC's management board had previously appointed a standing UK Crisis Management Team. As a result, within 2 hours of the fire starting the Team held its first meeting in a nearby building. Its leadership was of vital importance in the 24 hours after the disaster. The company's contingency plan was adhered to rigidly and it proved invaluable.

Despite the severe damage caused, all the company's major computer systems were running within 1 week of the fire, and some 470 employees had been found alternative accommodation across southern England.

Although the 14 central computers housed in the computer room were unharmed, they had to be taken out of service for cleaning, while some 450 terminals or workstations were either destroyed or damaged.

An inventory of hardware requirements was sent to managers at other DEC installations, and over 350 terminals and workstations were borrowed. This resulted in all major business applications running within 3 days of the fire. And in under 24 hours all data and voice communications links to Basingstoke had been re-routed to other DEC offices. The speed with which the operation of key business systems was resumed was due to off-site backups, alternative hardware and system compatibility. A procedure was in place to perform full system back-up to magnetic tape on a weekly basis, with tape copies being stored off-site and available at short notice. As the computer room was protected by a halon gas flooding system, many incremental backup tapes were saved.

The VMS operating system works over the entire VAX hardware range, so the transfer of applications from damaged computers to replacement machines was virtually invisible. In addition, DEC's private network is resilient based on a backbone network with alternative routing in case of a major problem. This built-in resilience ensured that communications could be re-routed quickly to other locations. Another benefit of DEC's networking architecture was that it did not restrict computer systems and their users to the same building, allowing greater flexibility in re-locating people and machines.

The case study illustrates the importance of :-

- taking control at a very early stage in the emergency;

- an effective contingency plan;
- adequately backed-up systems, with back-ups stored remotely;
- building flexibility and resilience into systems architecture to enable it to be adapted and/or replicated easily in an emergency.

2: Bombing - The World Trade Centre

In February 1993 a car bomb was detonated in a garage under one of the two 110 storey sky scrapers in the New York World Trade Centre complex. The complex, which houses some 900 businesses (including commodity exchanges, brokerage firms and banks), 50,000 employees and receives 80,000 visitors a day was thought to be "bomb proof", but no consideration had been taken of a portable bomb placed at a specific weak point in the structure.

The explosion :-

- took a number of television stations off the air;
- cut off electricity, telephone services, heating, ventilation and air conditioning;
- destroyed the police desk and operations centre;
- made the emergency power generation inoperable due to the water-cooling circuits being destroyed;
- made the CCTV and public address systems inoperable due to failure of the power supply.

It is interesting to note that a review of building security had highlighted many shortcomings in the WTC's emergency plans, but financial and 'other' considerations caused management to reject the findings.

The impacts of the explosion were widespread and severe. To give some idea of scale, one Japanese bank estimated that they alone had lost $20M a day in trading volume; the five commodity exchanges housed in the building are the source of annual revenues of $100M to the city and state treasuries, with overall estimates of revenue volume interrupted for the affected companies and government agencies reaching $1.07BN a month; and re-occupation of the offices in the tower was not possible until four weeks after the blast.

There were many lessons from this disaster. These included :-

- the building operator failed to have redundancy built into its emergency systems. They lost all control of voice communications and power since the emergency control centres were located in the impact area;

- a lack of adequate continuity plans affected many organisations. A survey subsequently showed that of the 200 companies interviewed, 90% lacked disaster plans and had no idea where to get backup facilities;
- the most mentioned problem was that of re-housing personnel. A wide variety of financial institutions scrambled to re-house their personnel in order to settle trades, participate in such markets as foreign exchange trading, and provide liquidity in bond markets. Extraordinary measures were taken to find work locations for people which included relocation in Toronto, London, Los Angles, and Frankfurt. In many cases, even where computer contingency plans were in place, little or no consideration had been given to the work issues;
- recovery of mainframe and minicomputer systems, where firms had adequate procedures developed over the years, most had failed to address fully the problems of LAN and microcomputer recovery
- backup media stored in basement of the WTC was damaged by smoke and water, while other backup stores located in the building could not be accessed;
- LANs accounted for most of the serious disruption. A number of companies used fault tolerant systems and tandem servers and their disruption was minimal, but others only backed their systems up weekly or monthly and their operations were greatly impeded. Several companies admitted to losing substantial amounts of data. Many did not have a workable backup system in place;
- microcomputers used as stand alone or in small networks sustained the greatest amount of damage in terms of system recovery. Few companies had formal backup policies, and many did not enforce them.
- The summary of issues learned, which focuses primarily on people issues, are :-
  - plan for business recovery in the very basic terms of where people will go to run the business. Arrange for space, ascertain who will be able to go where, make adjustments, test the plan, and keep it up-to-date (this is critical as the business and the IT support are constantly changing);
  - make sure that emergency accommodation is (or can quickly be) equipped with sufficient communications circuits (both voice and data) to link users with their systems.
  - the need for formal continuity plans which are appropriate to the risks the organisation faces and are workable. Whether or not a plan is workable can only be demonstrated by periodically testing it;
  - no continuity plan can be effective without data. Systems should be backed up sufficiently for them to be restored to operational use without first needing to be extensively updated. Backup copies should be stored at a secure remote location (in practice remote backup stores are rarely both remote and secure).

Summary based on articles in 'Computers & Security' magazine

3: System failure - UK national newspaper

A UK national newspaper were in the process of upgrading their computer equipment. Part of the upgrade involved selling an existing computer which had provided standby for an identical model which remained in service. It was this computer that caused the problem with a routine hardware failure. Engineers repaired the equipment which continued in operation for a day or two before breaking down again. Intermittent failures continued over a three week period during which the work of the accounts department fell further and further behind. Every time the computer failed, some 30 personnel could no longer perform their jobs because they were totally reliant on the computer. Although personnel worked overtime whenever the machine was available, this was not sustainable because they had other commitments and could not always work in the evenings or at weekends. Personnel morale began to decline due to the stop go nature of the work and the continual disruption to their private lives.

Both accounting and computer management's met regularly throughout the period to review the position. Eventually they decided to put their disaster recovery plan into operation. This involved the use of a "hot-site" at a computer bureau in central London. However, inadequacies in the plan showed up very quickly. All testing at the hot-site had been carried out by computer personnel, so users had never previously visited the bureau. Consequently, with the unfamiliar equipment and surroundings they were unable to achieve anything like the normal levels of productivity. Some programs needed to be adapted before they would run, and this further caused further delay. Finally, the capacity available at the hot-site was insufficient because the organisation's requirements had increased significantly since the recovery plan had been devised.

Thus, despite the move to the hot-site, work continued to fall further behind schedule. A further complication was that the deadline for payment of salaries was fast approaching, but the payroll system could not be run. Management therefore decided to draw up an action plan :-

- to obtain more computing capacity, particularly for payroll;
- obtain expert support;
- schedule all critical deadline;
- involve the Chief Executive.

The organisation were able to obtain more capacity by transferring part of their workload to another bureau while disaster recovery experts (provided by the company's auditors) provided valuable support.

It took a further month for the position to stabilise, although within that period the problems of having to management three sites in addition to their own premises placed a heavy burden on management. The organisation were fortunate that they were able to prevent a total disaster, because non-payment of their suppliers and personnel for a long period would have been very damaging to their business and reputation.

The lessons from this case study were that :-

- people problems need to be considered carefully. In particular, it is necessary to consider the affect of transferring them to unfamiliar locations and requiring them to work at evenings and weekends when this is not a part of their normal job;
- the affects of change must be taken into account. The continuity plan must be updated regularly to take account of changing business risks and requirements, and changes to the supporting IT systems;
- the continuity plan must be tested periodically, with the users participating as well as IT support personnel;
- top management are involved in the continuity planning process so that they can ensure that workable plans exist;
- systems should be ranked in order of priority - in this case the organisation considered that their payroll system was the most important to restore in the event of a disaster (they subsequently outsourced their payroll to a large bureau who could provide a level of backup that exceeded anything that the organisation could afford);
- management must take firm control of a potential disaster early before the damage is allowed to mount up.

4: System failure - UK local health authority

A DEC mini-computer was installed in a proper machine room set apart from other areas of the building. The machine ran unmanned for the majority of the time, but

required occasional software changes and other minor attention from an operator. A single operator was employed, and was also responsible for operating communications equipment.

Following a public holiday, the operator went to the machine room to restart the computer. He switched on, then loaded the disk holding the operating system. There was a loud grating sound from the disk drive, so the operator removed the disk and inserted the locally held backup disk on the same drive. Again this made a loud grating sound, so the operator took this disk out of the drive and mounted it on a second drive. This drive also made a loud grating sound.

By this time the operator was ware that there was a mechanical fault of some description, so he called for an engineer. The engineer found that both disks had been destroyed and both drives were beyond repair. The computer was out of action for seven days until new parts could be fitted. Some data was retrieved from the damaged disks by DEC, and some retrieved from off-site backup, but a large amount of data had to be re-entered.

The underlying cause of this failure was an attempt to save money, which in the long term proved to be a false economy. In particular :-

- the original problem was attributed to dust on the disk surfaces which was a result of a total lack of cleaning procedures in the computer room;
- an untrained operator who was unaware that the engineer should have been called at the first sign of difficulty, rather than spread the damage;
- the absence of an effective policy on backing up the computer.

5: Industrial action - UK Civil Service

During 1979 personnel working at a number of government computer centres were called out on strike in support of a pay claim. Dues were levied from trade union members to supplement the strikers' pay, and this strategy together with the union's careful selection of key computer centres helped them to inflict maximum damage.

The result was that there were delays in collecting hundreds of millions of pounds in government tax revenues, while the payments of government grants and subsidies to industry were halted, while payments to government contractors were delayed. Many other aspects of government, such as the production of new currency, state pensions payments and the processing of national statistics, were also affected. The result was that the bank minimum lending rate rose dramatically as did the government's need to raise revenue in the commercial money markets. At its peak some £1.4bn of government revenue and payments were held up.

After the strike had been settled the Civil Service formulated various plans to distribute computer processing, including facilities management and out-sourcing computer services to private contractors.

6: Flooding - Chicago Board of Trade

The Chicago Board of Trade Clearing Corporation process trade data and eighty other member brokerages. They had a disaster recovery plan which had been tested every three months. The following is a summary of the disaster that affected the Corporation in April 1992, when severe flooding occurred :-

- 9.20 am - the President of the Corporation declared a disaster. Twenty thousand people were evacuated from the area, and a power failure affected hundreds of buildings in the vicinity.
- 3.30pm - the Corporation re-located to temporary accommodation some 60 kilometres away, and resumed business.

At this point it appeared that testing had paid dividends because the disaster recovery plan worked and the Corporation were able to resume business activities. However, unforeseen problems started to emerge :-

- there were no facilities for the Corporation's customers to process their data because their buildings were flooded. To manage this problem the Corporation set up 30 terminals at another exchange and transmitted data; 35 other firms who had not been affected by the flood shared their facilities; and as soon as the power supply was restored, the Corporation converted their terminals to trading workstations;
- it was then discovered that there was insufficient printing capacity at the hot site which was producing over 1800kgs of documents daily on four laser printers. The Corporation hired helicopters to transport the hard-copy produced the 60 kms to their destination, but bad weather prevented the helicopters landing. So data communications equipment was flown in to the hot site to transmit the reports back to the Corporation's main building, which now had power partially restored.

The lessons that emerges from this case study are that a continuity plan :-

- must integrate with the needs of other dependant organisations;
- has not been properly tested unless it carries the complete live workload.

7: Lightning strike - UK local authority

A DEC mini-computer was installed in an office complex shared between a local health authority and a local council works department. The machine was used by the works department for payroll and administration and was located in a new purpose-built single storey building. The installation comprised the computer, modems and the legally required British Telecom line connection box.

During a violent thunder storm the computer room was struck by lightning. The lightning strike blew the line connection box from the wall, and a huge surge of current at very high voltage passed into the cables connecting the modem to the computer. This caused severe damage, although there was no fire because everything that was flammable had been charred by the lightning. Modems, cables and the backplane of the DEC were all destroyed, and only a printer was still useable. Even microchips within the DEC were blown out of their sockets.

There was minor damage to the building, but as copies of the software and data were held in a fireproof safe in another part of the site it was possible to restore the service very quickly using a computer loaned by a local education group under a long standing mutual contingency agreement. Damage was estimated at £100K, but only two days computing time was lost.

8: System failure - U.K. department of state

The Ministry commenced work on a project to replace their computerised accounting system and, following advice from consultants, engaged a small software house to Undertake the work. Following its delivery, the Ministry commenced a period of parallel running to prove the integrity of the new system but were unable to reconcile the outputs because of errors in the software.

Shortly after parallel running began the software house went into liquidation and at the same time the Ministry's existing system, which was no longer being manufactured, broke down irreparably. Since the old system was beyond repair and there was no back-up system, the Ministry had no option but to transfer their accounts to the new system even though it had not being fully tested and had known faults.

Serious accounting problems soon emerged, to the extent that the Ministry were unable to produce their usual monthly trail balances on the new system for seven months. The Ministry's accounts department were unable to resolve the problems, and extra staff had to be recruited to undertake a major exercise to rectify the errors. When the Ministry were eventually able to produce accounts for audit, they showed a net imbalance of £5.3M and included £26.4M which had been posted to "dump" accounts in their attempts to reconcile discrepancies.

This case highlights the risk of running an ageing system without backup. The Ministry suffered significant embarrassment, it was many months before they were able to regain sound financial control of their operations, and there was a significant cost in hiring additional personnel to correct the accounting and software errors.

9: Logic bomb : goods processing company

This company bought goods in bulk, split them up into small units, and added attractive packaging before offering them for sale. Although the firm was successful, margins were small and it was necessary to keep close control over the prompt allocation of goods to the several hundred production line staff. This task was carried out by a number of supervisors, who monitored orders taken, the arrival of incoming goods, and the flow of goods along the production line.

To help improve margins their margins, the firm commissioned a software house to develop a computer-aided production management system. In order to recoup the cost of the system, the firm made their supervisors redundant and gave them one month's notice. However, the new system was a month late in arriving, and the supervisors needed to be kept on for a further month. Shortly after they eventually left and the new system had taken control, a logic bomb destroyed its files. Because the data had not been backed up the new system could not be restored on another computer running modified software. As a result the firm's business activities came to a halt, they lost customers and eventually went into liquidation. Since the company ceased to exist there was no money to pay for an investigation, and the source of the logic bomb was never discovered.

Other than the obvious need to back up data at (appropriately) regular intervals, the other lesson to apply in this particular case was the need for an emergency manual system to fall back on in the event of the computer system failing. The firm worked a very tight order-processing schedule. Any significant break in service would result in them quickly losing custom to their competitors, which is what actually happened. Because of the nature of this incident, a fall back computer would not have helped, but the firm might have survived if they had been able to divert management from their usual tasks to taking over production line control.

10: Fire at Mercantile Credit

Churchill Plaza - facts and figures

Churchill Plaza is a 14 storey modern office block in centre of Basingstoke housing around 100 staff with medium size computer room and large PABX on the ground floor.

Fire started at 21.40 hours on Tuesday 16 April near the 8th floor wiring closet/office equipment area. Fire detected by smoke sensors, alarms sounded, and Fire Brigade arrived at 21.46 with 3 pumps. Fire spread rapidly to 9th floor and part of 10th floor by failure of external glazing and strong winds. Number of fire appliances and men engaged increased in several stages peaking to 30 pumps and 200 men. Fire fully under control by 0400 hours on Wednesday 17th April.

Selected senior management able to inspect most of building (although some parts of 8th/9th only from a distance) at 0700 hrs on Wednesday 17th April. 8th and 9th floor gutted, 10th partially damaged. 7floor serious smoke and water damage, 6th downwards heavily water damaged hence no power, head, light, water still running down walls, acrid smell. Main structure of building appears to have survived in good condition.

Recovery issues

- Situation - around 6 hours after fire put out (1000 hrs Wednesday).

Major Problems

- No power, heat or ventilation (Air conditioning), hence no computers.
- Main datacomms switches and master controller unusable (hence switching of circuits to bypass damage difficult).
- PABX - Working in battery backup mode.
- Two floors with around 100 PC's lost. The paper `backup' documentation was also lost, which meant several departments had no information, except that on the mainframe.
- A lot of other equipment (eg all photocopies) damaged by water.
- A PC & LAN sever backups kept in desks which were burnt (a number were retrieved and found to be usable).
- Much of the cabling (power, voice, data) damaged, difficult to verify whilst underwater.
- A lot of paperwork burnt or waterlogged (freeze drying can take a long time, and is expensive.
- Initial assessment bottom 6 floors could be made usable within 2/3 weeks, however some key functions needed to be working within a few hours. How could the 900 displaced staff be best used?
- Senior management fatigue beginning to set in.

Positive factors

- Main Computer Centre in North London unaffected (although switching of datacomms problematic).
- Branch Network and Northern Processing Centre in Manchester unaffected (all Churchill Plaza voice traffic was witched to Manchester from 08.00 on the Wednesday by BT, and their call rate increase from 1000 per day to 3000 per day).
- Local office with comms links (and a couple of DEC VAXs) 2 miles away used as a command centre and enabled 40/50 key staff (eg Treasury) to be working (in cramped conditions) by the Wednesday lunchtime.
- Plenty of spare office space and computer equipment available locally in Basingstoke (the recession has to bring someone good luck).
- TV and Radio coverage ensured we were not short of offers of help, however, responding the these offers, sorting "the wheat from the chaff" does take a lot of management time.
- As fire occurred at night no staff injuries or trauma of being evacuated in an emergency, hence lots of enthusiasm to assist in recover operations.
- Parts of ground and 1st floor just about habitable (for on site meetings) PABX worked (on standby power).

Action Committee Formed and Met Daily at 12.00

Key plan agreed

- Put as much work as possible into the branch network, and at the Northern Processing Centre. Where practical move some head office staff to work from local branches.
- Find new premises for 500 staff, and install desks, terminals, phones and comms links within 10 days.
- Plan to repopulate the better condition (lower) floors of CP from the second week at the rate of 2 floors per week (maximum that the logistics could cope with - eg number of heaters/dehumidifiers, rate at which cables can be laid & tested).
- Small teams of staff assigned to retrieve valuables (eg PC's, key documents) from the damaged building.
- Increase level of security, large numbers of usable, light pieces of equipment (eg calculators, dictaphones) were disappearing during the salvage operation.

Need to appoint a Loss Assessor (on our side) to take on the Loss Adjuster, whose role is to protect the interests of the Insurers.

Assistance From Vendors

> The timescales set were very ambitious, asking for items which normally take 3 months to arrive, to be delivered and installed within 4-6 days.

- Acceptable, vacant, local office space (unfortunately in 3 locations) was found and `signed up' in 24 hours. Barclays property Holdings obtained several hundred spare desks and chairs.
- BT provided 50 mobile phones and several FAX's within hours. Located and installed a 250 line/250 extension PABX in the main temporary building plus delivered multiple kilostream links within 5 days.
- IBM/DEC/Tandem/Data Logic/Computacentre all gave us priority with orders for Terminals/PC's/printers/controllers/processors etc, which started arriving in hours rather than days.
- To satisfy some demands we had 2/3 staff ringing round the brokers for several days and managed to clear out the UK stock of certain items (need to ensure disasters are scheduled and don't have several at once!)

- Local companies installed voice/data mains cabling at break neck speed (one building for 250 people completed within 48 hours).
- The loss adjuster insisted on a lengthy cleaning process for all the salvaged terminals and PC's. With excellent assistance from our suppliers/maintainers (Computacentre & Data Logic), several cleaning "production" lines were set up at their locations. Despite this we "lost" several hundred vital terminals & PC's for between 1 to 2 weeks, whilst the dismantling, cleaning, resembling and test procedures were followed through.
- Logistics control became a major challenge, as we could unpack PC's faster than we could wire in the power and comms links.

Reappraisal of Contingency Plans

What Went Well

In looking back to April, we are still impressed (surprised) at how well we did respond to a desperate situation.

- Contingency plan for loss of Datacentre easily adapted to cover loss of Head Office (eg provided a list of contact telephone numbers, and who takes what decisions).
- Contingency plan was up to date and accessible (probably luck in that we were due to do one of our twice yearly tests the following weekend).
- Staff enthusiasm (exciting adventure and also wanting to save the business) willing to work in difficult conditions (eg 90F, 100% humidity whilst building drying out).
- Reassured staff that the building is now safe (sent a video to each staff members home address).
- Rapid PR response, enabled damage limitation to public image, especially when the competition is mischief making!
- Branches and Northern Processing centre available and happily took up telephone traffic workload.

Lessons learned

- Don't keep PC backups in the desk drawer or filing cabinet (must be off site).
- Do have an up to date directory of home telephone numbers of key staff (who are they?) readily to hand.
- Avoid day to day use of important documents, use photocopies/microfilm etc instead.
- Have easily accessible copies of up to date site plans, plans of cable runs, power distribution etc.
- If you have a cable administration database, do have a backup copy offsite!
- No good having a sealed computer room with full Halon protection if your cable ducts are underwater.
- A hot standby computer system is not a lot of use if the end users have no terminals or telephones (or desks to put them on).

- Don't underestimate the damage water can cause (much of the cabling started failing 2/3 weeks after it was back in use due to corrosion, would have been best to replace the whole lot day 1).
- Is the Fixed Asset/Software register up to date?
- Computer Centre needed extra printing capacity as it was swamped by requested for reprints of historic reports.
- Need to appoint Loss Assessor day 1 to negotiate on an equal basis with the Loss Adjuster.
- Clear Desk Policy, large amount of paperwork left lying around can fuel a fire.

Finally (again) beware of over enthusiasm, and instant action, we for instance ordered the duplication of the same microfilm library at least twice!

FUTURE CONSIDERATIONS

Strategic Issues

A contingency plan is not just an IT problem, it should be on the Boardroom Agenda, be business lead and should raise a number of fundamental issues:

- encourage management involvement by use of Business Impact Reviews and polite reminders that there is an increasing legislation/Audit requirements for viable contingency plans to be in place;
- should the business be centralised in one location (lower cost, improved communications?) or decentralised into say a branch network (greater resilience);
- IT architecture, centralised mainframe (less popular nowadays, but at least the backups are usually actioned) versus PC's on a LAN?
- what is the real minimum contingency need, reassess importance of various departments in keeping the business alive (don't just assume the department with the most muscle/loudest voice is most important);
- what is contingency worth (10% of the profits?) If a central head office is vital, do you pay for a contingency empty office block 5 miles away;
- have you got the right type of Insurance Cover, don't assume the Landlord's policy is adequate, it won't for instance usually cover your increased cost of working;
- are you happy with the design of your main building? (eg open plan office layouts increase the rate at which fire spreads).

Planning and Testing Issues

Not a comprehensive list, but issues that have cropped up the "2nd and 3rd time of going around the loop".

Definition of a Disaster - what is included and what is excluded, the plan needs to state this - perhaps the kidnap of the chairman is not a disaster, but a strike and picketing of the company next door could be!

Assumptions - is the plan dependent upon say 50% of key staff being available? It is probably no longer sufficient to assume a friend down the road will provide you with "spare computer time" if you have a problem. How far away is the backup centre from the main centre, a few years ago ½ a mile may have seemed adequate, now I would suggest at least 5 miles.

Infrastructure Duality - at the construction/furbishment stage it is relatively cheap to equip a building for a secondary role - for instance cable (voice, data and power) a training school to handle large numbers of clerical/technical staff.

Modular Plans - the range of disasters that can occur dictate that Contingency Plans should be made modular, so that the relevant components can be selected for different scenarios. (Fire and Industrial Action probably require different responses).

Recognising a Disaster - a major fire is obvious, a gradual increase in the number of tape read problems at the datacentre is not. A standard fault reporting escalation procedure needs to be in place.

"War Games" are perhaps the ideal test (this is where the plug is pulled and half the staff announced "dead" without any pre-warning). However, unless the business is prepared for major disruption, they can have a serious impact and be career limiting. Datacomms are especially prone to being problematic.

User Involvement, vital, as their logistical needs are usually more demanding than those of the IT Department. Also user management involvement in tests is critical to gain their commitment. (If you are running a test over a weekend ring up the MD on the golf course to tell him how well it is going).

Return Home Activities - it is sometimes a lot easier to invoke your Disaster Contingency Service Supplier than it is to return home once the disaster is over. The Return Home requires a comprehensive plan, and needs to have the basics documented in the contingency plan.

10. Appendix 2: continuity plan pro-forma

Preface

This plan contains the information needed to restore an IT service following disaster at [insert location].

The plan is laid out in such a way that it should be easy to use in an emergency situation to facilitate initial recovery, and a controlled return of the IT service and customer service to normal.

Plan Updating

It is imperative that the plan is kept up to date. The Continuity Planning (CP) Manager is responsible for ensuring this by arranging regular review meetings and through formal change management procedures. More information on these subjects is available in the IT Infrastructure Library module on change management.

Amended pages or sections of the plan will be distributed to officers who have a copy of the plan. Destroy the pages replaced and insert the new pages. Note the change in the Amendment Sheet (A1.1). Update copies of the plan which are stored off site, and nominate a person responsible for ensuring this is done.

Distribution

The plan is in sections. This allows copying of relevant sections of the plan to officers, who do not need the complete plan. Treat the plan as a security document and as such control its distribution and access.

Copies have been distributed as follows:

Function	Sections

When a disaster Happens

The decision whether and, if so, how to invoke the disaster recovery action will be taken by the CP Manager, after assessing the situation and where necessary consulting senior management.

The actions to be taken by members of the disaster recovery team(s) to effect a recovery are contained in this plan. The programme of actions will depend on the length of time the disaster is expected to last, and the amount of damage to the installation. The CP Manager will notify which programme of actions is to be carried out.

How Serious is the disaster?

It is likely that separate programmes of action (see A1.4) will be devised to cater for different categories of disaster. Typically the severity of the disaster depends on the expected period of outage and the level of damage.

For example

Category	Outage	Damage
Minor	Up to 24 hours	Small
Medium	2-7 days	Partial
Major	more than 7 days	Severe

Introduction

This proforma plan is designed to help the CP Manager to design and produce a workable and comprehensive continuity plan. The proforma plan is a model which can be adapted to fit Departments' particular circumstances.

The proforma plan consists of proforma record layouts with notes for completion and advice on what other information should be included in the actual plan. It is not anticipated that every plan will contain all of the items, or categories, of information listed; discard redundant forms.

The contents of a continuity plan must contain all the information that the CP Manager needs to:

- decide the programme of action to be taken
- initiate the action
- control the continued processing of work as prescribed
- return the operation to normal.

Following a disaster the CP Manager needs to take advice form the teams (A1.3), and then decide on the length of time the IT service is expected to be out of action. Document A1.4 in the proforma plan, "When and how to invoke the plan", contains a list of the actions to be taken, depending on the length of time the service is expected to be unavailable.

Most of the detailed information required for the plan should already be available at the installation (eg Asset Register) or from the Initiation Stage (eg minimum computing facilities); see section 3.1 in the CP Module.

The proforma plan should be used in conjunction with the advice given in the CP module to develop a specific IT Continuity Plan.

Sections of the Continuity Plan

The Plan is divided into 7 sections.	**Page**
A1. Administration	**A-5**
This contains information on how and when to invoke the plan; the programmes of action to be entered into; the officers involved and where the emergency control centre is located.	
A2. IT Infrastructure	**A-17**
The hardware, telecommunications and software which comprises the replacement system and/or the reorder process are included, together with details of any contracts and agreements entered into in support of recovery and reorder.	
A3. IT Infrastructure Management & Operating Procedures	**A-21**
The instructions required to enable an IT (including DPU) facility to recommence operations following an emergency. Service level agreements are included in this section, and these include any relaxation of requirements that apply during a continuity.	

A4. Personnel	**A-29**
Contains information on the officers who transfer to the continuity site and of accommodation available to them if they are unable to return to their home because of the time and distance to be travelled.	
A5. Security	**A-31**

This section contains the fire and bomb instructions at the home site, and information on remote storage and the items stored there.	
A6. Continuity Site	**A-36**
This section is devoted to information about the location of the continuity site; the people to be contacted there; staff facilities; security; and of transport arrangements.	
A7. Return to Normal	**A-42**
This section states the dependencies which influence how return to normal can be achieved, and where possible how this is to be done.	

A1.1 Administration - Amendment Sheet

CHANGE No	DATE	Initials	CHANGE No	DATE	Initials

Use this form to record authorised amendments made to the document.

Initiate changes by the Department's change control system. Changes will also be initiated by the CP Manager through formal plan reviews (which are also subject to normal change control).

Insert the change number and the date on which the change is made, together with your initials.

A1.2 Administration - Incident/Action Log

DATE	TIME	INCIDENT	ACTION TAKEN	COVERED BY PLAN?:

Log any incident which causes, or occurs during, an emergency. Note the action taken; by whom; and whether the event had been anticipated and catered for in the plan.

The log contains

- a sequence of events in chronological order for reference and reporting purposes
- help for another officer to take control of the disaster recovery operation, if required
- information which can assist in any post-disaster reappraisal of the adequacy of the plan and possible revision.

The log must be produced by the Continuity Planning Manager (or his representative).

A1.3 Administration - Disaster Team

TEAM	MEMBERS	RESPONSIBILITY

To make the most productive use of staff in an emergency they should be organized into recovery teams and given specific areas of responsibility, and tasks to perform.

Typical teams, and their component members, should Include:

Management Team

- IT Services Manager
- Continuity Planning Manager
- Personnel Manager
- Finance Officer

Facilities and Security Team

- Configuration Manager
- Office Services
- Personnel Services
- Departmental Security Officer
- Welfare

IT Services Teams, under the direction of the IT Services Manager and the Continuity Planning Manger, as follows:

Operations Team

- Operations Manager
- Shift Leader(s)
- Operations/Technical Support

Telecommunications Team

- Network Manager
- Support Staff

Data Preparation Team

- Data Preparation Manager
- Data preparation Supervisor

Recovery & Service Quality Team

- Database & Software Recovery Manager
- Configuration Manager
- Change/Problem Manager
- User Liaison Manager
- Service Level Manager
- Help Desk
- Technical Support

The above list is not definitive and teams should be constructed to best suit the needs of the organisation.

For small organisations, combine a number of the tasks to be handled by a smaller number of teams, or even by one team, as appropriate.

Nominate substitutes for every team member, and inform them of their responsibilities in an emergency situation.

A1.4 Administration - when & how to invoke the plan

There is no proforma for this item.

The decision to implement the recovery programme is the responsibility of the Director of IT but may be delegated to the Continuity Planning Manager. The degree to which it is implemented depends on the severity of the break/disaster and the estimated time to restore the service. The sequence and timing of actions depends upon the criticality of the systems, be they on-line or batch. (An analysis of criticality is included in the Initiation Stage).

Produce a timetable of events showing the sequence of actions to be taken, depending on the estimated length of the loss of the system.

Subdivide the timetable to show

a) the immediate actions to be taken and

b) the longer term actions required to bring the home site back to normal.

The team responsibility for the action will also be shown.

Produce timetables for the three categories of disaster, examples of which are given in the Preface (minor <24 hours, medium 2-7 days, major <7 days). Examples of the first two timetables are given below.

EXAMPLE: TIMETABLE 1

The system is expected to be up and running again within 24 hours.

ACTIONS - IMMEDIATE	TEAM RESPONSIBLE
Place continuity contractors on standby	Management
Call in the engineers	IT Services
Establish whether to wait or go to the continuity site	Management
Inform Trade Union representative	Management
Inform users of situation (via Help Desk)	IT Services
If at any time during the 24 hour period the estimated length of the outage exceeds 24 hours go to the next Timetable	Management
When computer is operational again process outstanding work	IT Services
Take Continuity contractors off standby	Management

EXAMPLE TIMETABLE 2

The service is expected to be up and running again within 7 days.

ACTIONS - IMMEDIATE	
Call in the engineers	IT Services
Contact continuity contractors	Management
Proceed to continuity site	Facilities
Inform Trade Union representative	Management
Inform users (via Help Desk)	IT Services
Invoke Continuity Plan	Management
ACTIONS - LONGER TERM	
Plan return to home site	Management
Ensure SLA's maintained	IT Services
Maintain record of actions	Management
Record any processing backlog	IT Services
Release continuity contractors	Management
Pay continuity contractors	Management
Process backlog	IT Services
Review continuity plan	Management

The above are examples of timetables of actions to be carried out at particular times

Departments: produce your own timetables based on:

- the criticality of the estimated length of outage
- the team responsibilities
- the actions deemed necessary

The following are checklists of actions and responsibilities following an emergency.

MANAGEMENT TEAM

Move to the emergency control centre

Request an assessment of the problem (eg 999 services or security staff)

Contact the continuity contractors to place them on standby

Report to senior management (verbal)

Inform the recovery team leaders, and call a meeting to:

- ascertain the nature of the problem, the extent of the disruption, the consequences and likely implications
- agree team plans to be put into action immediately.

Act as main points of contact with emergency services and the media (via press officer)

Where the course of action is not obvious, allow an agreed period of time in which further information can be gathered in the severity of the problem and the likely period of outage.

Call another meeting to

- receive reports from team leaders
- decide whether to invoke the plan
- agree plans for each team to be reviewed at an agreed time.

Contact the continuity contractors either to arrange to use their services (eg a transfer to their facility), to update them on the situation or to release them.

- Initiate plans for transfer to the continuity site
- Report progress and plans to senior management

Following the move - at the continuity site:

- manage relations with contractors
- ensure the service levels contracted for with the users are provided
- ensure IT management procedures are adhered to
- monitor, and where necessary set in motion, plans for returning the processing to a permanent home site
- ensure any personnel problems are dealt with.

Following return:

- review the plan
- produce a final report to management
- oversee the work of the other teams; ensure they report back regularly; tackle any problems that they are unable to resolve for themselves.

FACILITIES AND SECURITY TEAM

Attend the initial meeting called by the Management Team

Attend to any staff problems resulting from the disaster

Conduct any asset inventory to include an evaluation of damaged equipment and equipment to be replaced, and update the configuration management database as necessary.

Make the site secure and carry out safety checks. Assess damage and time needed to replace accommodation and environmental services.

If the decision is taken to move to the continuity site:

- arrange hotel or other temporary accommodation
- arrange hiring etc of transport
- help with transfer of staff.

Following the move - at the continuity site:

- ensure all administrative support services such as typing, fax, telex, messengers, mail, office equipment are provided
- set up security procedures and access for staff (physical & logical)
- contact suppliers of essential services to connect supplies eg electricity, water, telephones
- provide any office supplies
- arrange for the transfer of media and other items from back up store to the continuity site and the setting up of another temporary back up site if required
- attend to any staff problems as a result of the move.

This team must prepare as soon as practicable, for the transfer back to the home site.

IT SERVICES TEAMS

Consult with computer engineers.

Attend the initial meeting called by the management team.

Contact all operations, operations/technical support, data preparation, data control, job control and output handling staff:

- to appraise them of the problem and the initial actions being taken
- to make sure they know what to do.

Inform users, via the help desk, of the problems and the plans for informing them of a resumption of service.

If a decision is taken to move to the continuity site:

- contact suppliers of replacement machinery and ancillary equipment. Inform them of the move and order equipment
- brief all staff who are to transfer to the continuity site
- arrange with the Facilities and Security Team the transfer of staff and essential documentation to the continuity site, and the backup media and other items from the backup store.

Inform users of the current situation.

Following the move - at the continuity site.

In conjunction with the Facilities and Security Team, monitor the delivery and installation of any equipment.

Accept handover of the facility after initialising and testing the hardware, operating system and telecommunications networks (in conjunction with other teams).

Prepare production schedules

Take security copies of all files before commencing processing.

Transfer security copies to new temporary backup site.

Recover the service and start processing of work in accordance with the schedule. Ensure technical support are on hand to iron out any problems.

Ensure infrastructure management disciplines are maintained (eg performance and serviceability monitoring, capacity, change, problem and security management). Ensure service level agreements are honoured.

This team will need to schedule the processing of any backlog of accumulated work following transfer to the continuity site (and on return to home site).

The preceding paragraphs contain detailed check lists for the teams that are likely to have heavy involvement in the work associated with a disaster, and the recovery from it. Departments; adapt these to fit your own situations.

Identify additionally other functions (eg admin) as necessary, set up teams and produce check lists of actions and responsibilities they have to carry out.

A1.5 Administration - emergency contacts (internal)

NAME	ORGANISATION/ RESPONSIBILITYI	TELEPHONE No		HOME ADDRESS
		Office	Home	

List the name, section and telephone number of officers within the building or organisation for ease of communication:

- security
- engineers
- electricians
- heating/aircon engineers
- Office Service
- first aid
- welfare

A1.6 Administration - personnel who have a copy of the plan

NAME	LOCATION	PHONE No	RESPONSIBILITY	SECTIONS HELD All/Part Only

Generate a list of officers who have a copy of the plan. If a copy of the plan is destroyed or is rendered inaccessible by an emergency this list will make it easier to acquire a replacement copy. Keep a number of up-to-date copies stored in a secure location off-site in case the disaster results in access to the building, or parts of it, being denied.

Use the list to serve as a distribution list for amendments.

A1.7 Administration - location of emergency control centre(s)

LOCATION	ADDRESS	TEL No

In the event of a disaster, set up an Emergency Control Centre (ECC) for the Continuity Planning Manager and the Management Team to meet there as soon as the disaster occurs. Direct all activity and communication from the ECC throughout the disaster and undertake from there the work needed to return to normal.

This centre is about controlling the disaster, not managing the continuity site.

Ensure the ECC is easily accessible, secure, and as close as possible to the affected facility. Give consideration to locating an ECC close to the home site but, where possible, in a separate building. Where the ECC is located at the home site, Departments should make provision for an alternative control centre in case the main one is not available.

Ensure the ECC is fully equipped, with normal office facilities including telephone(s). Store copies of the plan securely in the room at all times.

File a map of the location of the ECC here.

A2.1 IT Infrastructure - service contractors

NAME	ORGANISATION & Service Provided	TEL No	CONTACT

List service contractors and maintenance companies which may be contacted to supply services or equipment associated with recovery.

- computer equipment suppliers
- telecomms equipment suppliers
- data entry equipment suppliers
- software suppliers
- output processing
- machinery removal
- equipment cleaning
- accommodation cleaning
- off site media and/or plan storage
- hot site provider
- cold site provider
- processing/data entry bureau.

A2.2 IT Infrastructure - asset register

There is no proforma for this item.

Ensure the installation's asset register is available from the configuration management section. Further information on asset registers is available in the IT Infrastructure Library module on Configuration Management. Use this register to help the reorder process for hardware damaged or destroyed together with any necessary software.

Include:

- computer hardware
- telecommunications equipment
- data processing equipment
- output processing equipment
- software, including version numbers

If a minimum configuration would be an acceptable way to proceed for an interim period, direct attention to the next section.

A2.3 IT Infrastructure - minimum computing facilities

There is no proforma for this item..

These are the facilities required, hardware, software and telecommunications to provide an interim service, based on processing only the critical applications on a smaller system. This information is/has been used to identify suitable continuity services available and/or to order replacement facilities.

Use the same layout as the asset register for this purpose.

See A3.1 for configuration details.

A2.4 IT Infrastructure - contracts & agreements

There is no proforma for this item.

File copies of all contracts and agreements relating to existing or replacement items here.

Include:

- hot start suppliers (fixed & portable)
- cold start suppliers (fixed & portable)
- bureau(x)
- dormant contracts (if used)
- software licence agreements.

A3.1 IT infrastructure management & operating procedures - IT infrastructure management

There is no proforma for this item.

Ensure all IT Infrastructure Management procedures and support documentation are available at the continuity site (eg service level, change, problem, configuration management. See specific IT Infrastructure Library modules for more details).

A3.2 IT infrastructure management & operating procedures - service level agreements

There is no proforma for this item.

Copy and file all Service Level Agreements here. It is possible that special conditions apply in a continuity situation; include details of these in the SLA.

A3.3 IT infrastructure management & operating procedures - operations manual

There is no proforma for this item.

Ensure the Operations Manual reflects the conditions as they obtain at the continuity site, and include instructions on:

- powering up and down
- system loading and unloading
- peripheral configuration
- peripheral handling and cleaning
- media handling
- system breaks/incidents and what to do
- scheduled/unscheduled maintenance
- environment monitoring eg what to do when the power trips out or the air conditioning fails
- network map & necessary strappings
- anything else which will be different for Operations at the continuity site.

Ensure the manual contains copies of all computer, data preparation and network configurations. (NB Give special consideration to configuration details when minimum computing facilities are being used).

A3.4 IT infrastructure management & operating procedures - processing schedules

There is no proforma for this item.

Note: these schedules already exist if the complete workload is being transferred to the continuity site, but produce a selected subset if only the critical work is to be processed.

Carry out any recovery work required when work is transferred to a continuity site, particularly if media have been damaged or destroyed. The amount of recovery depends on how often the files are backed up and the amount of work done since the backup. Include instructions on how to carry out this recovery task in this section. When that recovery task is complete, schedule the work to run in its proper sequence.

These schedules will have been produced to the Department's own standards and layout.

A3.5 IT infrastructure management & operating procedures - service/job operating instructions

There is no proforma for this item.

Ensure a copy of the Job Operating instructions exists for each service/job which is to be run at the continuity site (see the Continuity Planning module section 4.1 for further details).

Include information on:

- input
- parameters
- console messages, and how to respond to them
- restarting
- magnetic media
- expected output
- output handling
- support any procedures & contacts.

Include copies of end-user procedures/notices that are different in a continuity situation.

A3.6 IT infrastructure management & operating procedures - data entry procedures

There is no proforma for this item.

Reproduce any specific procedures for inputting data into the system, including direct data entry via terminals or PCK only if they are not included as part of separate job instructions.

Produce separate data entry procedures if a Data Prep Bureau is to be used in a continuity situation (see A2.1 and A2.4).

A3.7 IT infrastructure management & operating procedures - output processing

JOB	FORM NO/ OUTPUT IDENTITY	QUANTITY	PAPER/OTHER PROCESS

If special handling processes are required, detail them here.

Note: this is particularly important if processing of output:

- is to be transferred to a bureau
- is to be handled at a site away from the computer processing
- where the job operating instructions cannot be released eg for security reasons.

A3.8 IT infrastructure management & operating procedures - clerical procedures

There is no proforma for this item.

Input copies of any clerical procedures which are to be used as an alternative to, or to complement, computer systems here, similarly if jobs already exist which require an element of clerical work eg job preparation and submission.

A4.1 Personnel - officers transferred to continuity site

NAME	GRADE	JOB	LOCATION AT CONTINUITY SITE	
			Room	Tel No

List those officers to be transferred temporarily to the continuity site to provide a useful record:

- for Personnel and pay purposes
- for arranging transport
- for ease of contract
- to assess if sufficient personnel are available following the disaster
- for security purposes.

Wherever possible, attempt to identify the exact individuals (eg where shift workers are involved) and ensure that tasks to be carried out and the staff numbers involved are detailed.

A4.2 Personnel - accommodation/hotels etc

TYPE OF ACCOMMODATION	ADDRESS	Tel No	CHARGES

Where residential accommodation is required provide a list of suitable establishments, with maps showing where they are located. Usual sources for this information are tourist information offices and/or people working at the continuity site.

Assign the Facilities and Security Team responsibility for booking accommodation in an emergency situation, after first checking the type, and cost, required.

A5.1 Security - fire & bomb instructions

There is no proforma for this item.

Insert a copy of the fire and bomb instructions telling staff what to do, and where to go, when the alarms are sounded.

A5.2 Security - first aid

There is no proforma for this item.

Provide instructions on the first aid/medical facilities available including:

- names and locations of trained officers
- location of "rest" room
- location of medical supplies
- first aid during shift working.

Insert the instructions here.

A5.3 Security - emergency service contacts

NAME	ORGANISATION/RESPONSIBILITY	TEL No

Insert here the names of public utilities and departments which may be contacted to provide emergency action with the names of individuals if known, and where to contact them:

- Fire Service
- Police
- Medical Services (including hospitals)
- Electricity
- Gas
- Water
- Drainage
- BT/Mercury
- PSA
- Insurance
- Air Conditioning Maintainer.

A5.4 Security - location of/access to remote stores

COMPANY/ROOM/SAFE	ADDRESS	CONTACT	TEL No

Record the location of any company, or other departmental facility, used for the security storage of items, together with a map of the location.

A5.5 Security - items stored at remote site

ITEM	DESCRIPTION	QUANTITY	MEDIA IDENTITY

Record the items stored remotely as follows:

Backup media

A record of the tapes and discs copied regularly, with discmaps and filenames etc to facilitate identification and transporting to the continuity site.

Stationery

The types of stationery and quantities stored.

Computer cleaning materials

It may be necessary to store such materials, particularly if they are not available at the continuity site, or they cannot be obtained quickly.

Blank media

If blank media is needed eg for carrying out security copying at the continuity site.

Replacement equipment

If spare items of kit are stored remotely.

Documentation

Copies of the continuity plan, source code listings etc.

A6.1 Continuity site - location

NAME **ADDRESS** **Tel No(s)** **FAX No** **E-Mail** **BUS ROUTES(S)** **STATION** **LOCAL CAB Tel No(s)**	

Write all information on where the site is and how to get there here, together with a map showing the exact location and points of entry and any special requirements to gain access eg security pass, telephone authority.

A6.2 Continuity site - contacts

NAME	TITLE/SECTION	Tel No	ROOM No

List all permanent officers at the continuity site, who may need to be contacted:

- to arrange testing
- for information relating to their procedures
- immediately after a disaster.

A6.3 Continuity site - staff facilities

FACILITY	DETAIL

Provide those facilities which are essential for staff in any workplace eg washing and toilet facilities, heating and lighting and also certain minimum space requirements.

Provide the following facilities for the convenience of staff at your continuity location:

- vehicle parking
- restaurant/canteen facilities
- recreation facilities.

If staff are expected to work and stay at a location some distance away from their normal office, then include information on service and facilities available at or near that location here.

A6.4 Continuity site - security

There is no proforma for this item.

Ensure these instructions are available:

- entry to the building
- entry to controlled areas
- access to systems
- emergency procedures including fire and bomb warnings and evacuation procedures
- first aid facilities.

A6.5 Continuity site - transport

TYPE OF VEHICLE/PURPOSE	COMPANY	Tel No

Provide transport as required for carrying:

- staff
- media
- supplies
- mail
- input/output.

Record the type of transport required and the companies which can provide the services.

A6.6 Continuity site - people/items to be transported

PEOPLE/ITEMS	QUANTITY/ NUMBER	WHEN	FROM	TO

Record the people and other items which will need transporting, how often eg daily, weekly, once only and the pickup and putdown locations.

A7 Return to normal

EXTENT OF DAMAGE	PREDICTED DURATION OF OUTAGE
PROPOSED CORRECTIVE ACTION	**RESPONSIBILITY**

Note that the guidance given in the module states that returning to normal largely depends on a number of things which can not be predicted. However enter here what actions can be planned with certainty in advance, for each of the timetables previously mentioned (eg minor <24 hours, medium 2-7 days, major >7 days).

Actions depend on:

- extent and nature of disaster (how much damage)
- duration of outage
- processing of backlog.

After returning to the home site, the Continuity Planning Manager will conduct a review of the continuity operation, assess the effectiveness of the plan, instigate any changes to it, and report to senior management.

Example

EXTENT OF DAMAGE	**PREDICTED DURATION OF OUTAGE**
Total destruction of IT installation by fire	18 months
PROPOSED CORRECTIVE ACTION	**RESPONSIBILITY**
Immediate	
Clear site	Building Services
Salvage machinery	Office Services
Dispose of scrap machinery	Office Services
Reappraise equipment needs	IT Strategy Group
Reappraise accommodation needs, human/equipment	IT Strategy Group
Redesign building	Building Services
Tenders for new buildings	Building Services
Supervise new building work	Building Services
Some time later	
Acquire equipment	Contracts Branch
(Retrain)staff	Training/hardware supplier
Site trials and handover	IT Services Manager
Transfer services from continuity site	IT Services teams