Building a **Business Continuity Plan**

GUIDELINES FOR PREPARATION OF YOUR PLAN

AIG

Building a Business Continuity Plan

A disaster is defined as “any unplanned event that results in the inability of the business to support operations in whole or in part”. A business is vulnerable to three different types of disaster:

- **Natural disasters**
- **Wilful damage**
- **Accidental damage**

To minimise the damage to the business by such an occurrence, it is necessary to have a recovery plan, which addresses the worst case scenario – destruction of the building or main facility. See Appendix A for listing of potential disasters.

BUSINESS CONTINUITY PLANNING GUIDELINES

No matter what the size of the business, similar principles will apply:

- A senior person in the business should take ownership of the business continuity plan. The plan should be allocated the same importance in business planning as, for example quality management, cash flow or health and safety
- The responsibility of managing the business continuity plan must be clearly established within the business and everyone should know the importance of the plan and who has overall responsibility
- A small team of suitably qualified and/or experienced people should be assembled to review the business operations and itemise the key features and areas of operation
- The scope of the work must be established. An organisation may already have, for example, adequate recovery plan for its IT system. Such a plan would however need to be included in the completed Business Continuity Plan
- It is imperative that a business is able to respond to any type of emergency. A disaster or emergency situation is, by definition, unexpected. The business continuity plan should be prepared along the following principles:
    - The plan should have a broad scope if it is to effectively address the many disaster scenarios that could affect the company.
    - It should not distinguish between a partial loss of service and a complete loss of services and facilities. A “worst case scenario” should be the basis for developing the plan - destruction of the main or primary facility.
    - Because the business continuity plan will be written based on the above assumptions, less critical situations can be handled by using only the needed portions of the plan, with minor (if any) alterations required.

This document identifies broad issues that should be addressed in your planning. It is recommended that you read through all the items first, before starting. A checklist has been provided for each of the three phases highlighted above. The purpose of the checklist is to assist the team when preparing a business continuity plan. It should be filled in as the planner progresses through the process of developing, documenting, and implementing the business continuity plan.

Components of a Business Continuity Plan

A business continuity plan is a working document that reflects the business as it is and not as it was. It should be concise and easy to use. The procedures state what tasks should be done, but not necessarily how to carry them out. The reason such specifics are avoided is that a successful business continuity plan requires the flexibility to be creative, within a given situation, and not be encumbered by strict compliance and detailed procedures. A business continuity plan should identify decisions (including options) to be made during a disaster.

There are three stages to creating a business continuity plan:

i. Conduct a risk assessment and an analysis of the impact on the business in order to determine the magnitude of the exposure to threats
ii. Develop and document the business continuity plan
iii. Test, approve, and implement the business continuity plan. This stage includes maintaining the business continuity plan on an ongoing basis to meet the changing demands of the business.

Stages	**Objective**
I. Risk Assessment	
1. Risk Evaluation	➢ Identify critical business functions essential for continued service or production. ➢ Determine the events that can adversely affect your company, the damage that such events can cause and the controls needed to prevent or minimise the effects of a loss potential.
2. Business Impact Analysis	➢ Identify the impacts that result from disruption that can affect the company and the techniques that can be used to quantify and qualify such impacts. ➢ Prioritise critical business functions.
II. Develop and Document Business Continuity Plan.	
1. Develop Recovery Strategy	➢ Determine and guide the selection of alternative recovery operating strategies to be used to maintain the critical functions.
2. Document Plan	➢ Organise and document a written plan. Senior management should review and approve the proposed plan.
III. Test, Approve and Implement Business Continuity Plan.	
1. Test Plan	➢ Develop testing criteria and procedures. Coordinate, test, and evaluate the plan. Document all results.
2. Approve and Implement Plan	➢ Obtain senior management endorsement of plan.
3. Maintain Plan	➢ Develop processes to keep the plan up-to-date with reviews and tests completed at a maximum of 12-month intervals. ➢ Ensure the plan is in-line with the strategic direction of the company.

I. RISK ASSESSMENT

1. Risk Evaluation - Identify Critical Business Functions

This part of the process is aimed at identifying those processes and functions that are critical to the operation of the business; the speed that the impact of their loss will be felt and within what time-scale.

Critical business operations are generally those which do not have scheduling flexibility. Initially entire departments or operational areas may not be needed. These departments may however become critical depending on the duration of the emergency. Therefore, the time frame of when a function becomes critical should also be considered. It may be useful to allocate to each operation a time frame within which the impact would begin to be felt: for example this may be within 4 hours, within 24 hours, within 1 week. When planning, it will help to list the critical functions and the managers/people in charge of them. (See Appendix E for sample of blank template.)

The following items should be reflected in the critical business section of the business continuity plan.

- Identify the position(s) and employee(s) responsible for each function
- List the employees' home, mobile and work phone numbers and address in case mail is necessary
- List the resources needed for each critical function. Consider the minimum necessary for continued operations
- Identify any variances in the time of year for critical functions (i.e. temporary help employed every November and December to assist warehouse staff etc.)
- Identify any variances in resource needs
- List alternate sites for a complete loss of services, include: space needed and contact for alternate site (home, mobile and work phone number)
- Document your means for relocating personnel safely
- Identify how you will relocate equipment
- Document who is responsible for relocation logistics; include their home, mobile and work phone numbers
- Document alternative (back-up) methods for relocating people and equipment. Plan to use the minimum number of people and equipment for restoring critical business functions. Include an alternate person for logistical responsibility

2. Business Impact Analysis - Identify Risk and Impact on Business Functions

- All business operations must perform a risk and business impact analysis. Based on the level of risk associated with the functions performed, a recovery plan may be required. The risk analysis should be updated at least annually and after any major system or operational change which has resulted in a material effect on the risk associated with a given operation.
- One method for determining the risk associated with an activity is to document all the functions performed by each department. Once the primary functions have been identified, the operations and processes should be ranked in order of priority: essential, important and non-essential.
- Recovery Priority - For every product or service provided by the business unit / function, list and describe the impact to the business assuming all resources (personnel, equipment, etc.) become unavailable. Critical business functions should be prioritised according to their impact on day-to-day operations.

  For example

Classification	Description	Recovery Time Frame
Priority A (Essential)	Functions absolutely essential to remain operational	Up to 48 hours after disaster declaration
Priority B (Important)	Functions that are critical and should be performed in a timely manner following the completion of priority “A” functions	3 – 7 days after disaster declaration
Priority C (Non-essential)	Functions that enhance operations but are less time critical for the company to remain operational.	8- 30 days after disaster declaration

- The importance of some functions will vary depending upon when the disaster occurs. For example, accounting and tax-related functions are generally tied to statutory or regulatory deadlines, etc.

Quantitative impact

- Assess the quantitative impact of the loss to the business. If an area provides a support function and loss of the process or service would primarily impact other business functions, the quantitative loss impact will be based on the dependent business operations.
- State the duration of the impact. It is up to the business unit to determine the definition of short, moderate, and long-term as they pertain to the business product / service. For example, short term may be one day, moderate term one week, and long-term one month.
- Describe the impacts of the loss of the business product / function and estimate the qualitative impact. Quantify using the following ranges of values, the loss for each of the impact time value.

Example:

1.	Less than £10,000	per duration
2.	£10,000 – £100,000	per duration
3.	£100,000 – £500,000	per duration
4.	£500,000 – £1,000,000	per duration
5.	£1,000,000 – £2,500,000	per duration
6.	£2,500,000 – £5,000,000	per duration
7.	£5,000,000 – £10,000,000	per duration
8.	£10,000,000 – £50,000,000	per duration
9.	£50,000,000 – £100,000,000	per duration
10.	Over £100,000,000	per duration

(See Appendix F for sample of blank template.)

II. DEVELOP and DOCUMENT BUSINESS CONTINUITY PLAN

The previous work will have identified the organisation of the business; the risks facing it and the potential damage to the business. Management must decide on which level of risk is acceptable to the business as this will help determine the actions to be taken and how the Business Continuity Plan will be developed.

The options are:

1. Accept the current situation.
2. Reduce the likelihood and /or the impact of the disaster to a more acceptable level.
3. Eliminate or reduce the potential effects to a negligible level.

The first option relies on the ability to recover from the event quickly. The analysis and assessment exercise will have identified the dangers likely to be encountered, however by the time recovery has been completed customers may have found alternative suppliers.

The third option can involve considerable expense.

The second option is often the preferred one as the exposure of the business is reduced as far as reasonably practicable and the consequent effects lessened. The Business Continuity Plan then details the manner in which the remaining risk will be managed.

1. Develop Recovery Strategy

Identify Communication Channels

- Specify what other locations, departments and personnel will need to be contactable during an emergency.
- Identify what you might need to discuss or communicate
- Indicate personnel that will need to be accessible
- Determine how you will communicate. What might be done if there are no telephones immediately available to you or the other party? Set your alternatives in order of priority and document it. You may want to consider two-way radio for the most important members of your emergency management team
- Indicate how your employees will be notified of an emergency during non-working hours. If you plan on using radio stations, it is recommended that you arrange for two stations. Prior arrangements with radio stations are usually necessary
- Determine when you will need to communicate with people managing the critical operations - at the start? …continually?...intermittently?
- Indicate any differences in time you will need to communicate with your staff or with foreign countries as this will affect your communication plans (i.e. USA, Europe, etc.)
- Consider media press statement and appoint a designated spokesperson

Identify Necessary Resources

- Document the minimum number of personnel needed for critical functions
- Decide who is needed to perform the critical functions. Aside from the managers you named earlier, who else might be need and how many (or how few) people will be needed?
- Consider what will be need to perform the critical functions in terms of alternate manufacturing, warehousing and office space, computer hardware, operating systems, files, telephones, etc. Think in terms of minimal amounts
- Decide how you will obtain the requisite material and from where (supplier, warehouse, factory, off-site storage)? Do not rely on only one supplier. Establish alternate sources of supplies wherever possible
- Indicate when these items will be needed. Will they be needed at all stages of a relocation, at the beginning, or at the end?
- The most practical alternative for maintaining production or services in case of a disaster should be researched and evaluated. It is important to consider all aspects of the company

- Recovery alternatives may include:
  - Manufacturing assistance;
    a) within the company
    b) third party manufacturers
  - Alternate warehousing and distribution facilities
  - Hot sites for computer services
  - Reciprocal agreements
  - Multiple computers
  - Service centres
  - Consortium arrangement
  - Suppliers of
    a) equipment
    b) raw materials
    c) services
  - Combinations of the above
- Detail equipment needed at each of the alternate sites
- Specify what equipment is available at each alternate site
- Identify the means for getting additional equipment that will be required
- Indicate time frames for equipment needs
- Identify all contacts for equipment needs (i.e. manufacturers, wholesalers, agents.). List their home, mobile and work telephone numbers
- For a listing of data gathering materials and documentation that should be maintained see Appendix D

Disaster Decision Making

- Determine which teams will be needed before, during, and after a disaster takes place. A good starting point is to envision the chain of events after a disaster occurs or during an emergency

  See Appendix B for a listing of teams that may be created
- Identify the members of the decision-making teams. Include home, mobile and work numbers for each team member and home addresses in case mail is necessary
- The role and responsibilities of each team should be addressed at a high level. The specific tasks that each group will be responsible for completing, such as building evacuation, power back-up issues, notification of authorities, notification of employees, should be defined
- At what point in time should this chain of command or team take effect?
- Propose locations where a team could be based
- Every team member should have at least two copies of the applicable parts - one in his / her desk and one at home. The idea is to be able to act quickly while reducing confusion. This kind of working document is to be updated as needed, and at the least, annually

Disaster Assessment

- Define what constitutes a major disaster for your operations (e.g. a loss of services for more than 3 or 5 days). What, in your opinion, constitutes a disaster for the business? Describe what you consider as the difference between a minor set back and a disaster
- How would the extent of an emergency be assessed?
- Describe / list your sources and locations of information and where you will get information, for disaster assessment and for returning to normal operations
- Identify who is needed to make assessments about the disaster?

Create Accelerated Access Plan

Any condition that delays the return to normality, such as prolonged inability to re-enter the disaster area, carry many cost with them. Tangible costs include loss of income, wages, and assets. A well conceived and executed "access plan" will ensure that the right people can quickly enter the right areas at the right time.

2. Document The Plan

- Poorly written plans are difficult to use, quickly outdated, and can be extremely frustrating. Well-written plans reduce the time required to read and understand the procedures and therefore, result in a better chance of success if the plan has to be used. Well-written plans are brief and to the point
- A certain writing format should be employed when writing the plan. A standard format for the procedures should be developed to facilitate consistency and conformity throughout the plan. Standardisation is especially important if several people write the procedures
- If any aspect of the plan is based on certain assumptions, write them down. Throughout the attached checklist, the planner is reminded to document all assumptions. See Appendix C for a list of common planning assumptions
- If the planner encounters difficulty in preparing the plan, it may pertain to the fact that he / she is trying to plan for areas that he/ she should not be planning for. You cannot do someone else's plans. This exercise should be departmental-driven. The departmental managers need to determine what their critical functions are, and who the people are that are needed to perform those functions

III. TEST AND IMPLEMENT BUSINESS CONTINUITY PLAN

1. Test Plan

- Develop testing criteria and procedures. Procedures to test the business continuity plan should be documented
- Perform testing. It is essential that the plan be thoroughly tested and evaluated on a regular basis (at least annually)
- The plan should be updated to correct any problems identified during the test
- Types of tests include:
  - Checklist tests
  - Simulation tests
  - Parallel tests
  - Full recovery / interruption tests
- The tests will provide the company with the assurance that all necessary steps are included in the plan. Other reasons for testing include:
  - Determining the feasibility and compatibility of backup facilities and procedures
  - Identifying areas in the plan that need modification
  - Providing training to the team managers and team members
  - Demonstrating the ability of the company to recover
  - Providing motivation for maintaining and updating the business continuity plan
- If certain functions within the company are out-sourced / processed by a third-party (i.e. spray painting, electro-plating, distribution) management should:
  - Evaluate the adequacy of the third party's business continuity plan.
  - Ensure that the company's business continuity plan is compatible with the respective third party's plan.

2. Approve and Implement Plan

- Once the business continuity plan has been written and tested, the plan should be approved by top management. It is top management's ultimate responsibility that the company has a documented and tested plan

- Develop a plan to implement the business continuity plan. Adequate training should be provided for personnel within the company that will have business continuity responsible for major functions (i.e. damage assessment, logistics, facilities, restoration, etc.)

3. Maintain Plan

- Procedures should be developed to review the impact of new processes, systems and technology on a regular basis. (i.e. quarterly, half-yearly, annually)
- Document all changes to the original business continuity plan

CHECKLIST FOR ANALYSIS

The planner should complete the checklist to ensure that all components of a business continuity plan have been addressed. Each section should be completed as the planner proceeds through the three-stage process. It is based on the preceding Business Continuity Planning Guidelines.

CHECKLIST FOR ANALYSIS

Submitted by:	
Company/Department Name:	

Plans for **Critical Operations**

	Y/N
1. Critical process / functions listed?	
a) Accompanied by the position responsible for the function?	
b) Employee names for each position and alternates?	
c) Employees' phone numbers and address in case mail is necessary:	
Home?	
Work?	
Mobile?	
d) Identified resources needed for each critical operation?	
e) Prioritised the operations to be maintained and how to maintain them?	
f) Is outsourcing an option?	
g) Identified what other functions / departments will be impacted or rely on your department / process?	
List assumptions made:	

2) Is there any variance in the time of year that process / function is critical?	
a) If so, any variance in positions responsible?	
➢ Employee names?	
➢ Employee phone numbers	
Home?	
Work?	
Mobile?	
b) If so, any variance in resource needs?	
c) Resources identified?	

3) Alternate sites listed:	
a) Listed for complete loss of service in geographic area.	
➢ Space required?	
➢ Contacts and phone numbers?	

4) Methods of relocating:	
a) Personnel?	
b) Equipment?	
c) Name of person responsible for relocation logistics?	
➢ Phone number?	
d) Alternatives listed?	

List assumptions made:	

Risk and Impact Analysis

	Y/N
1) Identified and prioritised critical business operations /functions?	
2) Assessed quantitative loss for each business operation / function / product / or service?	
3) Described the impacts of the loss of the business product / function?	
4) Defined impact time duration?	
5) The following items have been addressed in determining risk and impact analysis: I. Considered impact on loss of income? a) Delay in billings b) Delay in cash flow c) Loss of sales d) Loss of expected future business II. Considered loss of assets? III. Considered impact on loss of customers? a) Negative media coverage b) Loss of competitive edge c) Loss of good will IV. Considered additional cost? a) Increased operating cost b) Loss of discounts on payables c) Penalties on late delivery d) Cost of legal and regulatory actions	

Communication Channels

	Y/N
1) Identified name of contact and specified when to contact? a) Do you need to contact major suppliers, customers, third parties? b) How will customers be notified of new business location or alternate site? Specify what other departments and personnel your department will need to contact.	
2) Identified topics for discussion?	
3) Identified way of notifying employee a) radio ~ pre-arranged? b) TV ~ pre-arranged? c) others ~ pre-arranged?	
4) Identified means by which critical staff will be contacted during non-working hours (e.g. home telephone numbers, beeper and cellular telephone number)?	
5) Prioritised method of communication? If yes, what is the priority? ➢ telephone ➢ Mobile ➢ fax ➢ computer on-line ➢ modems (dial-ins) ➢ courier others	
6) Have samples of communications to be disseminated in a disaster or emergency (i.e. media release, radio broadcast, letter to customers, employees, etc).	

	Y/N
7) Above done for: a) partial loss b) complete loss on site c) complete geographic loss	
8) Variance in times for need to communicate	
List assumptions made:	

Necessary Resources

	Y/N
1) Determined number of personnel needed for critical operations / functions?	
2) Determined manpower requirements for weekend and overtime processing.	
3) Identified hard copy documents which are vital to the company and not able to be recreated (files, contracts)	
4) Machinery, plant & equipment identified? Created checklist of required resources	
5) Identified equipment needed at each alternative site?	
6) Identified equipment available at each alternate site?	
7) Identified means for getting necessary equipment?	
8) Indicated time-frame for equipment needs?	
9) Identified phone numbers of all contacts for equipment needs	
10) Ensured business continuity plan manual is updated, stored off-site, and accessible.	
List assumptions made:	

Disaster Decision Making

	Y/N
1) Created organisational chart which groups personnel into business continuity team (contact / notification team, staff monitoring team, recovery team, damage assessment team, risk management team etc.) Defined the responsibility for each member of the team (primary and coordination).	
2) Created a list, in descending authority order, of people permitted to authorise emergency measures.	
3) Identified members of the decision making team? a) Phone numbers ... Home? Mobile? …Work? b) Home address in case mail is necessary.	
4) Identified when team should take effect? Identified the maximum time which can lapse before the recovery plan and team must be put into operation.	
5) Identified location for team to meet during emergency and when they should meet? a) Have supporting information such as maps, transportation routes, location, etc. b) Identified housing arrangements for the firm's recovery team (hotel, corp. apartment, etc.)	
6) Business continuity instructions are stored off-site in an accessible place known to employees needing to get hold of the plan.	
List assumptions made:	

Disaster Assessment

	Y/N
1) Major disaster defined?	
2) Minor disaster defined?	
3) Method of assessment identified?	
4) Information sources identified?	
5) How do you determine that the disaster is over?	
6) Notified employees when and where to return to work after a disaster strikes?	
List assumptions made:	

Accelerated Access

	Y/N
Developed an accelerated access plan?	
List assumptions made:	

Write the Plan

	Y/N
1) Business Continuity Plan documented?	
2) Business Continuity Plan approved by senior management?	
List assumptions made:	

Test the Plan

	Y/N
1) Designed and documented procedures to test the recovery plan?	
2) Developed schedules for testing recovery plan, in whole, and in part?	
3) Provided training to team members and employees?	
4) Testing allows sufficient time to re-test any component of the plan that should fail.	
5) Developed procedures to document the results of the test.	
6) Documented the successful completion or failure of the test.	
7) Updated the plan to correct any problems identified during the test.	
8) Evaluated adequacy of service bureau / third party / supplier's business continuity plan.	
List assumptions made:	

Maintain the Plan

	Y/N
1) Formal review of plan scheduled for predetermined intervals (i.e. quarterly, semi-annually, annually, etc.)?	
2) Developed procedures to review the impact of new processes / systems / system enhancements / procedures and policies?	
3) Established policies, procedures, and responsibilities for reviewing recovery plan at required interval/s?	
4) Documented results of formal review?	
List assumptions made:	

APPENDIX A – TYPES OF DISASTERS / THREATS

This list is for example only and is not exhaustive

Natural

- Internal flooding
- External flooding
- Seismic activity
- High winds
- Snow storms
- Tornado
- Hurricane
- Epidemic
- Volcano
- Tsunami

Wilful

- Bomb threats
- Terrorism
- Civil disorder
- Sabotage
- Explosion
- Biological contamination
- Hazardous waste
- Work stoppage / strikes (Internal/External)
- Computer crimes
- Arson.

Accidental

- Chemical spills
- Radiation contamination
- Power failure/fluctuation
- Heating, ventilation or air conditioning failure
- Telecommunications failure
- Gas leaks
- Impact by vehicle or aircraft
- Breakdown
- Explosion
- Fire

Consider also denial of access or damage to facilities as a result of an incident not on your site or directly affecting your facilities.

APPENDIX B – TEAM APPROACH

The team approach is used in developing a plan as well as recovery from a disaster. The teams have specific responsibilities and allow for a smooth recovery. Within each team a manager and a deputy should be designated. These persons provide the necessary leadership and direction in developing the sections of the plan and carrying out the responsibilities at the time of a disaster.

In addition to the recovery management team other potential teams might include:

- Departmental recovery teams
- Computer recovery team
- Software team
- Damage assessment team
- Security team
- Facilities support team
- Administrative support team
- Logistics support team
- Off-site storage team
- Communications team
- Human relations team
- Marketing/Customer relations team
- Accelerated access team
- Other teams

Various combinations of the above teams are possible depending on the size and requirements of the business. The number of members assigned to a specific team can also vary depending on need.

Each team has specific responsibilities that must be completed to ensure successful execution of the plan. The teams should have an assigned manager and a deputy, in case the team manager is not available. Other team members should also have specific assignments where possible.

The recovery management team is especially important because it coordinates the recovery process. The team should assess the disaster, activate the recovery plan, and contact team managers. The recovery management team also oversees, documents, and monitors the recovery process. Recovery management team members should be the final decision-makers in setting priorities, policies and procedures.

APPENDIX C – PLANNING ASSUMPTIONS

The following is a list of common assumptions that should be used to heighten the planners' awareness of the issues involved and allows the company to take any necessary actions. This list of assumptions is not all-inclusive, but is intended as a thought provoking process at the initial stage of planning. The assumptions themselves will often dictate the make-up of the plan; therefore, management should carefully review them for appropriateness.

General Assumptions

- The main facility of the company has been destroyed
  - The assumption is made that the office will be accessible to retrieve files and other equipment. This may not be the case. Note - accelerated access does not override any life safety issues.
- Staff is available to perform critical functions defined within the plan
- Staff can be notified and can report to the backup site(s) to perform critical recovery, and reconstruction activities
- Off-site storage facilities and materials survive
- The business continuity plan is current
- Subsets of the overall plan can be used to recover from minor interruptions
- Surface transportation in the local area is possible

Data/Systems Assumptions

- Data Back-ups
  - Only on–site back-ups are sufficient.
  - Another company location or third party will provide data back-up for mainframe systems.
- LANs
  - Data can be retrieved even with the loss of the site.
  - Dial-in capability to other LANs from alternate sites.
  - Overall assumptions that these issues can be handled when the situation arises instead of making detailed prior arrangements.
- Hot site locations will be provided by a third party.
- Overall assumption that hardware (PCs, printers, etc.) will be easily obtained when needed.
- Access to various systems will be possible from alternate sites.
- A third party is prepared to coordinate systems re-routing.
- Tailored software will need to be altered in order to run alternate sites.

Communication Assumptions

- Telephones
  - Will be available
  - Fax lines or E-mail are the next best alternative.
  - Single phone line supplier (i.e. BT) is adequate.
  - Reliance exists on suppliers for telephone equipment, alternate sites and any other communications needs.
  - Cellular phones are set-up as back-up to phones.
  - Phone "hotlines" can be set up for employees to call for information concerning a disaster.
  - PBX system will remain operable to retrieve messages.
  - Operators will be able to re-route calls.

- The most effective plans will provide for the worst possible situation. Therefore, your plan should assume that communication via telephones (and/or fax and modem lines) may not be possible (at least in the first stages of a disaster). Alternative communication means can be cellular telephones, walkie-talkies, or CB radios. Be aware that cell-phone networks may be unavailable due to heavy usage in the immediate aftermath of an incident such as terrorism.
- Local network news can be used to inform staff of the status of a disaster.
- The company's telecommunications department will (or should) have re-routing plans for all lines and phone numbers to predetermined locations.
- The company has established a communication link to disseminate information throughout the group
- Communication can be carried on through other regions' LANs

APPENDIX D – DATA GATHERING ITEMS

Recommended data gathering materials and documentation that should be maintained includes:

- Critical telephone numbers (customers, suppliers, broker, insurer, agents, etc.)
- Communications inventory (number of cellular phones on hand, etc.)
- Distribution register
- Documentation inventory
- Machinery inventory
- Plant inventory
- Office supply inventory
- Main computer hardware inventory
- Microcomputer hardware and software inventory
- Insurance Policy inventory
- Master call list
- Master supplier list
- Notification checklist
- Off-site storage location inventory
- Software and data files backup/retention schedules
- Temporary location specifications
- Other materials and documentation

APPENDIX E – TEMPLATE

Definition of Critical Business Function, Products and Services

Business Unit_____ Date Completed_____

Preparer Name, Title, Phone Number: _____

Business Function Name	Description of Key Products / Services Provided	Human Resource Dependencies

APPENDIX F –TEMPLATE

Impact of Loss

Business Unit / Function _____ Date Completed _____

Prepare Name, Title, Phone Number_____

Business Product / Service_____

Duration of Loss	Quant. Impact	Description of Impact of Loss	Equipment / Resources Needed	Application

APPENDIX G –BUSINESS CONTINUITY PLAN GUIDELINES

Phase 1Incident Control

A Procedures

- ❑ Ensure emergency evacuation plans are well organised, publicised and practised
- ❑ Regularly review procedures for evacuation assembly, temporary shelter and accounting for all personnel
- ❑ Formulate instructions for notifying emergency services
- ❑ Consider alternatives for communications, transport access and employee welfare

B Information

- ❑ Create and maintain site plan indicating:

  Fire hydrants and emergency equipment
  Isolating points for utility services
  Hazard materials, chemicals etc.
  Building configuration and layout
- ❑ Prepare call out list of essential personnel and telephone numbers, including specialist damage control contractors
- ❑ Nominate senior person for dealing with communications for employees, trade unions, statutory authorities, insurance, corporate office and press
- ❑ Arrange for technical liaison with emergency services

C Reporting

- ❑ Delegate a senior person for collating information and evidence relative to the incident for investigating purposes
- ❑ Record all information and times of response actions for post incident evaluation

D Equipment

- ❑ Inform and train employees to use available emergency equipment
- ❑ Prepare action plans for closing down and isolating plant, machinery & processes

Phase 2Reinstate Business

A Facilities

- ❑ Compile a building and property list indicating critical dimensions
- ❑ Maintain an agency list for leased and saleable property
- ❑ Compile a register of all plant, equipment, tools and consumables
- ❑ Establish list of potential suppliers of plant, equipment, tools and consumables
- ❑ Evaluate potential use of facilities at other Company locations
- ❑ Identify any legal, planning or environmental constraints

B Services

- ❑ Measure minimum consumption requirements and specialist constraints of utilities and mains services
- ❑ Record suppliers of portable emergency equipment
- ❑ Register list of specialist contractors

- ❑ List vehicle hire companies for road vehicles & material handling

C Equipment

- ❑ Identify and record specifications of critical, unique or specialist plant and equipment
- ❑ Determine sources of temporary or permanent supply & availability for plant & equipment

D Procurement

- ❑ Maintain update lists of specialist contractors, suppliers & agencies
- ❑ Formulate authority & approvals procedure for emergency finance acquisition, expenditure and control
- ❑ Identify potential consultants and services e.g. design, construction, demolition, statutory approvals

E Communication

- ❑ Determine level of authority for press communication
- ❑ Prepare procedure for informing & liaising with employee, client, customers, corporate staff, Insurance & Statutory Authorities

F Records

- ❑ Ensure availability of critical data, information, records and documents
- ❑ Arrange alternative methods of processing information and data
- ❑ Organise the recording of all information and evidence of incident conditions for insurance and investigation purposes

www.aig.co.uk

BELFAST
Forsyth House
Cromac Square
Belfast BT2 8LA
Tel: 02890 726002
Fax: 02890 726085

BIRMINGHAM
Embassy House
60 Church Street
Birmingham B3 2DJ
Tel: 0121 236 9471
Fax: 0121 233 3597

CROYDON
2-8 Altyre Road
Croydon
Surrey CR9 2LG
Tel: 020 8681 2556
Fax: 020 8680 7158

GLASGOW
Centenary House
69 Wellington Street
Glasgow G2 6HJ
Tel: 0141 303 4400
Fax: 0141 303 4440

LEEDS
5th Floor Gallery House
123-131 The Headrow
Leeds LS1 5RD
Tel: 0113 242 1177
Fax: 0113 242 1746

LONDON
58 Fenchurch Street
London EC3M 4AB
Tel: 020 7954 7000
Fax: 020 7954 7001

MANCHESTER
4th Floor,
201 Deansgate
Manchester M3 3NW
Tel: 0161 832 8521
Fax: 0161 832 0149