

# **Business Continuity Planning and Self Assessment Guide for Professional Risks**



## CONTENTS

### Business Continuity Planning Guidance

		Page
1	Introduction	3
2	The Disaster Recovery Team	4
3	Preparing a Plan	5
	Step 1 - Service Levels	5 - 6
	Step 2 - Risk Analysis	6 – 14
	Step 3 – Emergency Action Planning	14 – 16
	Step 4 – Business Recovery Planning	17 – 19
	Step 5 – Testing and Maintaining the Plan	19 – 20
4	Documentation and Copies	20
5	Further Information and Guidance	20

### Business Continuity Planning Self Assessment

Planning Forms
Checklists
Contact Lists

#### IMPORTANT NOTICE

This document has been developed by Aviva Risk Management Solutions which has made extensive efforts to check the accuracy of the information and advice contained in this document and it is believed to be accurate at the time of printing. However Aviva Risk Management Solutions make no guarantee, representation or warranty (express or implied) as to the accuracy or completeness of any information or advice contained in this document. All advice and recommendations are presented in good faith on the basis of information, knowledge and technology as at the date of publication of this document.

Without prejudice to the generality of the foregoing, Aviva Risk Management Solutions make no guarantee, representation or warranty (express or implied) that this document considers all systems, equipment and procedures or state of the art technologies current at the date of this document.

Use of or reliance upon this document or any part of its content is voluntary and is at the user's own risk. Anyone considering using or implementing any recommendation or advice within this document should rely on his or her own personal judgement, as appropriate, seek the advice of a competent professional and rely on the professional's advice. Nothing in this document replaces or excludes (nor is intended to replace or exclude) entirely or in part mandatory and/or legal requirements howsoever arising (including without prejudice to the generality of the foregoing any such requirements for maintaining health and safety in the workplace).

Except to the extent that it is unlawful to exclude any liability, Aviva Risk Management Solutions accept no liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from the publication of this document or any part of it or any use of or reliance placed on the content of this document or any part of it.

# BUSINESS CONTINUITY PLANNING GUIDANCE

## 1. INTRODUCTION

Various surveys on business resilience have been conducted by the Home Office and organisations such as the Business Continuity Institute. They all confirm that an 'unthinkable' disaster can happen and when it does it may cause healthy businesses to fail. Planning makes a substantial difference to the likelihood of surviving an incident, particularly when:

- The likely impact of significant events on the business has been assessed
- The response to these events have been planned
- The effectiveness of the plan has been tested and revised where needed
- Time, thought and, where necessary, money is invested in managing risk.

The process, which is targeted at producing a clearly defined and documented Plan, basically has two aims.

- To minimise the risk of a disaster happening
- To maximise the ability to recover should a disaster occur.

Insurance plays its part, but many of the effects of a disaster such as damage to your brand or image may not be insurable and it therefore pays to make appropriate plans in advance.

All businesses are different and it is therefore not possible to create a generic template that applies in its entirety to every business. However the self assessment guide we have developed can be tailored to most small to medium sized professional and office type businesses, for example by:

- Expanding or adding to the checklists.
- Amending or expanding the Business Continuity Plan Objectives and Procedures on [Form B](#)
- Adding an Executive Summary to include a Company Policy Statement and Recovery Objectives. This demonstrates to staff that a Business Continuity Management process has been introduced and that measures are in place to enable the business to begin to return to full capacity. As part of this summary, predefined timescales can be given against the identified measures/activities so everyone is clear what needs to be done in the first 24 hours for example
- Creating detailed Departmental Contingency Plans, for example to facilitate the recovery of IT Systems. These plans, whilst important in their own right, are not a substitute for preparing a full Business Continuity Plan which looks to protect the business as a whole. They can therefore be added to the main plan as appendices. If they are not attached to the plan they must be accessible in the event of an emergency.

To help illustrate the Business Continuity Planning process, we have included a series of examples for a hypothetical company - XYZ Recruitment Consultancy Ltd. These examples will be shown in green text.

Where there is an action to be taken to create your Business Continuity Plan, this will be shown in blue text. [Hyperlinks](#) allow you to navigate directly to the appropriate [Forms](#) and back again, simply by placing the cursor on the appropriate [Form](#) and pressing the Ctrl button + click.

## 2. THE DISASTER RECOVERY TEAM

Developing and implementing a plan is best done by a team. The Disaster Recovery Team should be made up of managers and staff that are able to work effectively in challenging circumstances and can adapt to a changing situation. Deputies should also be identified who can cover for absent team members.

The team members should, between them, have a good understanding of all business areas including operations and processes, legal, finance, HR, IT, premises, client management, publicity, health & safety, fire and security precautions. It is important, at the outset, to ensure that the team has a common understanding of the company's primary business objectives. This will avoid disputes over priorities at a later stage in the planning process.

A Disaster Co-ordinator should be appointed to lead the team and to decide when it is necessary to invoke the Business Continuity Plan.

It important to remember, when selecting the members of the disaster recovery team, that there will need to be others outside the team who can continue to manage the parts of the business that have not been affected by the disaster.



Depending upon the size of the business and the number of locations it may be necessary for the Disaster Recovery Team to be supported by individual, departmental or location teams.

[Form A - Disaster Recovery Team contact page](#) has been supplied within this document for you to record the members of your company's disaster recovery team.

### 3. PREPARING A PLAN

When you have selected your team they can follow the 5-step process below to create a Business Continuity Plan.



#### STEP 1 – Service Levels

The Disaster Recovery Team must agree on a statement of core business objectives (see [Illustration 1](#)). This is not about the systems in place to support the business, but a statement of what the business does and who it does it for.

Start by asking yourself: “What is it that my business basically does?” Achieving a common understanding of the company’s primary business objective is essential at this stage. This is ultimately what the Business Continuity Plan is being designed to protect and recover. Your Business Continuity Plan will fail at the outset, if the participants in the plan differ in their basic view of what the business exists to provide.

Ensure your senior management sponsors agree with this statement. [Copy this statement onto Form A of the Template.](#)

Having defined the Core Business Objectives the business must also understand its “normal level of service” i.e. what it aims to deliver to its customers and stakeholders every day. It must also understand what its “minimum acceptable service” is i.e. the essential service it has to provide to avoid immediate permanent loss of custom, reduce possible financial penalties and fulfil its primary contractual obligations. Please see [Illustration 1](#) below [and then complete Form B Service Levels Log](#)

### Illustration 1 – Example Statement of Core Business Objectives and Service Levels

XYZ Recruitment Consultancy Ltd

**Core Business Objective:** *To provide recruitment services (permanent positions) to the UK civil engineering sector with a particular specialism in transport projects.*

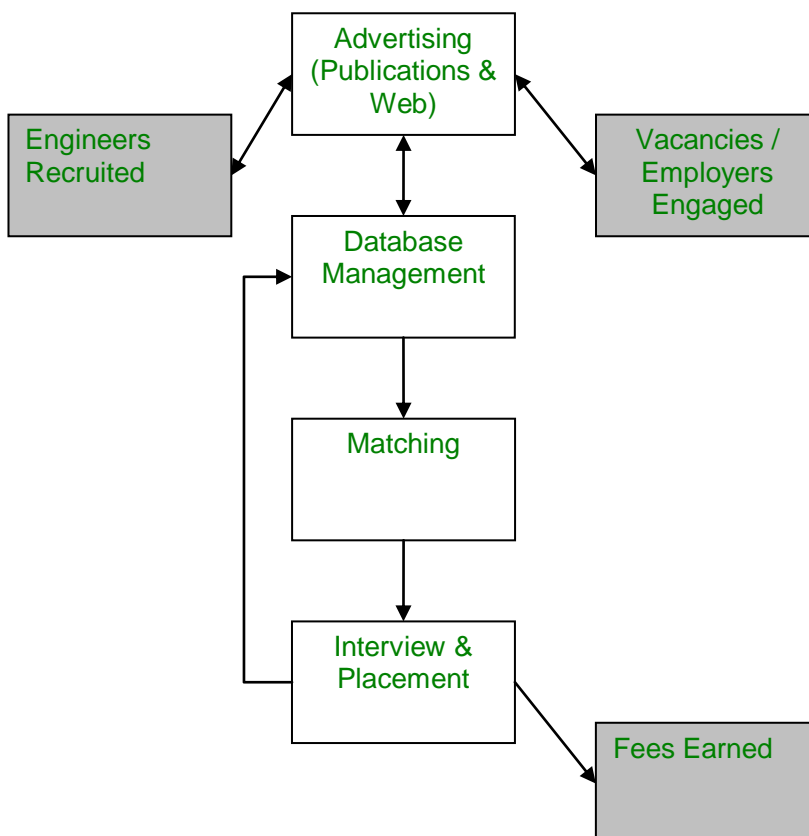
**Normal Service Level:** Maintain an up-to-date database of engineers; maintain contact with employers; maintain an up-to-date database of vacant positions; advertise in 3 x monthly and 8 x weekly publications; update vacancies on own website on a daily basis; arrange interviews within 48 hours of request.

**Minimum Service Level:** Update transport engineers in database once a week; update database of vacant positions on a weekly basis; advertise in monthly publications; update vacancies on own website on a weekly basis; arrange interviews within 72 hours of request.

### STEP 2 – Risk Analysis

As well as understanding the “Normal Service Level”, it is essential to understand how the business operates to achieve this on a day to day basis. Business can be viewed as a set of linked processes. Some of these ‘Business Processes’ have a greater bearing on the core activities of the business than others. Those that have the greatest or strongest relationship to the core activities are often referred to as ‘Critical Business Processes’. **Illustration 2** shows a very simple model of our recruitment consultants. The basic processes and functions illustrated are those which simply have to be in place for the company to fulfil its primary objective. You may find it helpful to create a simple model of your own business along these lines.

### Illustration 2 – The XYZ Recruitment Consultancy



The plan should ensure that your business never falls below your minimum service level and that your recovery to the normal level of service is achieved in the shortest possible time.

To ensure this, you need to understand what each of the functions / departments in the business has to deliver to support the minimum service level. This can be done by means of a workshop, interviews or questionnaires to key personnel. Consider using or amending [Form C](#) if you want to conduct a questionnaire process. [Illustration 3](#) shows the output from such a process and the requirements falling upon each departmental function.

**Illustration 3 – Examples of Departmental Functions within the XYZ Recruitment Consultancy Co and support required from them to meet Minimum Service Levels**

- Advertising
  - Ability to amend adverts / web presence to align with business requirement of meeting minimum service levels
- Client Relationships
  - Access to Transport Engineers Database
  - Access to Employer Database
  - Immediate contact with Transport consulting engineering practices and daily progress updates
  - Contact Transport Engineering applicants within 2 days and update weekly
  - Contact within 7 days to all other employers and update weekly
  - Contact all other engineers within 7 days and update when normal service resumes
- Database Management
  - Entry of engineers and employers
  - Vetting of applicants
- Matching
  - Access to Transport Engineers Database
  - Access to Employer Database
- Interview and Placement
  - Access to Transport Engineers Database
  - Access to Employer Database
  - Production of placement & contract documentation
- Admin services supporting the above e.g.
  - Facilities
    - Arrange temporary / alternative premises
    - Provide office equipment
  - HR
    - Contact own staff to advise of revised working arrangements
  - Finance
    - Arrange emergency funds
    - Resume payment processing (in/out) within 7 days
    - Continue payroll processing within 2 days
  - Legal and compliance
    - Maintain records of ingredients traceability
    - Ensure all H&S legislation complied with
  - I.T.
    - Systems in place to ensure the above timescales are met

Use the output of this exercise to consolidate the results and transfer these to the Critical Business Processes Log on [Form D](#) provided. You may also want to record who is normally operationally responsible for the process and then decide which member of the Disaster Recovery Team will be responsible for this process if the plan is invoked. Where a process or resource is shared, it should be made clear which Team Member will have the necessary responsibility.

Risk Analysis is the process of recognising the threats that face your business (risk mapping), understanding what the consequences of these threats occurring would be (business impact analysis) and then putting protection and mitigation measures in place to ensure that you will always be able to provide your minimum level of service whatever happens (risk reduction).

**Question:** What is a risk or threat?

**Answer:** Anything with potential to adversely affect the business whether they are technical, economic, internal, external, human or natural. An extensive but not exhaustive list of potential threats to a business is shown below. Many may not be appropriate to your business, whilst there may be others not listed which could apply.



*Adverse weather conditions*  
*Aircraft impact*  
*Arson*  
*Assault*  
*Bankruptcy of customers*  
*Bankruptcy of suppliers*  
*Boiler failure*  
*Bomb threat*  
*Breach of duty of care*  
*Breach of Health & Safety regulations*  
*Breach of regulatory requirements*  
*Breach of contractual conditions*  
*Cash flow interruption*  
*Civil disturbance*  
*Computer failure*  
*Computer virus*  
*Damage to brand, reputation, corporate image*  
*Defective structures*

*Denial of access*  
*Disgruntled employees*  
*Earthquake*  
*Electricity failure / shortage*  
*Emerging public health risk / epidemic / pandemic*  
*Equipment loss/ breakdown/ damage*  
*Explosion*  
*Failure of alarm systems*  
*Failure of fire protection measures*  
*Failure of maintenance standards*  
*Fire*  
*Flood*  
*Fraud*  
*Gas leakage*  
*Gas supply failure*  
*Hazardous local events*  
*Hot work*  
*Ignition sources*

*Illicit smoking*  
*Inadequate insurance*  
*IT loss/ breakdown/ damage*  
*Labour relations*  
*Lightning strike*  
*Location*  
*Loss of records*  
*Negative publicity*  
*Pressure group protest*  
*Public transport interruption*  
*Security failure*  
*Skills shortage*  
*Storm damage*  
*Strike*  
*Subsidence*  
*Telecomms failure*  
*Terrorism*  
*Theft*  
*Trespassers*  
*Troublesome neighbours*  
*Vehicle problems*  
*Water damage*  
*Water supply*

There are several ways to analyse the risks facing your business. We have chosen a simple and straightforward method of assessing Risk and providing a Rating for your business. You may need to seek further advice if your business has complexities or specialisms which are not compatible with this method.

Some of those identified for the XYZ Recruitment Consultancy Co are shown below in [Illustration 4](#)

## Risk Rating Method

Using the [Risk Analysis Form E](#) provided:

- Choose the top threats facing your business using your knowledge of premises, location, processes and trade specific factors. Consider what effects these risks would have individually on the critical business processes you have already identified in [Form D](#) and, where necessary, the effects on the business as a whole (e.g. where there are separate buildings on a site the threat of fire may need to be considered separately for each but the threat of flood would apply across the whole business at the site).
- For each risk identified, it is necessary to consider likelihood and significance to ascertain its risk rating. The formula and definitions are shown below:

$$\text{Risk Rating} = \text{Likelihood (1-4)} \times \text{Significance (1-4)}$$

### Definitions

- **Likelihood:** *the chance of a threat occurring*
  - 1 = never known to have happened in the business sector or locality
  - 2 = known to have happened in the business sector or locality
  - 3 = known to have happened once in the company
  - 4 = known to have happened more than once in the company

Likelihood depends upon reviewing past experiences within the company, other businesses in the area, the trade sector you are within and any other special circumstances which might affect the probability of an incident occurring. It should also take into account existing protection measures which are in place.

- **Significance:** *the degree to which the business is affected*
  - 1 = no significant effect
  - 2 = disruptive but not affecting most trading / service provision
  - 3 = disruptive and affecting most trading / service provision
  - 4 = catastrophic / destructive
- The higher the rating the more exposed the business is and the greater the need for risk reduction and business continuity planning.
- Consider undertaking a separate analysis for failure of protection measures where required (e.g. failure of automatic fire detection systems).
- Transfer the results to the [Form F - Business Impact Analysis Matrix](#) (by typing into the appropriate box) as shown within [Illustration 4](#) for the XYZ Recruitment Consultancy Co. This will help you identify and prioritise where risk mitigation / risk improvement measures may be required.
- The management of the business will have to decide if the risk rating for each threat is acceptable to the business. If this is not, then further risk reduction measures may need to be implemented to reduce the risk rating to an acceptable level. This should be recorded in the [Risk Analysis Action Log Form G](#). The timescale may be influenced by budgetary constraints, but if a threat appears in a red box you may need to review your budget.

#### Illustration 4

#### Example of XYZ Recruitment Consultancy Co Ltd Risk Analysis Exercise

Top Threats identified for the company are:

- Loss of IT due to software virus
- Loss of IT due to hardware failure
- Denial of Access

##### **Identified threat – Loss of IT due to software virus**

**Likelihood: 4** – Known to have happened more than once in the company – this has happened twice in the last 6 months. The business is a heavy user of email and is therefore exposed to viruses entering the system via email

**Significance: 2** – Disruptive not affecting most trading – The IT Manager has found software patches to remedy the situation within 48 hours.

**Risk Rating:** Likelihood 4 x Significance 2 = Risk Rating 8. This is assessed as amber – room for improvement.

The decision is taken to install anti-virus scanning software on the email server to provide protection against such virus attacks. After this risk mitigation was implemented the risk rating changed to 6 (Likelihood 4 (unchanged) x Significance 1 (reduced) = Risk Rating 4). This changes the risk rating to Green.

##### **Identified threat – Loss of IT due to hardware failure**

**Likelihood: 3** – Known to have happened once in the company. A critical component failed during overnight backup 12 months ago.

**Significance: 3** – Disruptive and affecting most trading. It took 1 day of investigation to identify the faulty part, 2 days to obtain a replacement and a further day to install the component and a further day to install and re-commission the system. During this period the company was not able to access several of its core systems and had to rely on sparse paper records.

**Risk Rating:** Likelihood 3 x Significance 3 = Risk Rating 9. This is assessed as amber – room for improvement.

The company has decided to improve its maintenance regime and enter into contract for replacement hardware with an IT hardware recovery provider. After this risk mitigation was implemented the risk rating changed to (Likelihood 2 as a result of the maintenance contract (reduced) x Significance 1 as a result of the IT hardware recovery contract (reduced) = Risk Rating 2). This changes the risk rating to Green.

##### **Identified threat – Denial of Access**

**Likelihood: 2** – Known to have happened in the business sector or locality. A body was found in the basement of a building in which a competitor had an office. The police denied access to the building for 36 hours whilst scene of crime investigations continued.

**Significance: 3** – Disruptive and affecting most trading. Although closed 2 business days, overtime was used to catch up with work over the next week, however the business missed out on the renewal of a major contract.

**Risk Rating:** Likelihood 2 x Significance 3 = Risk Rating 6. This is assessed as amber – room for improvement.

The company could not identify any practical risk mitigation measures, and therefore decided to ensure such an incident would be covered by means of insurance.

**Illustration 4 continued**

**Risk Analysis Form**

	Threat	Mitigation Measure	Likelihood (A)	Significance (B)	Risk Rating (A x B)	Red / Amber / Green	Action (Y / N)
1	Loss of IT / virus	None	4	2	8	Amber	y
2	Loss of IT / virus	Anti-virus software installed	4	1	1	Green	N
3	Loss of IT / hardware failure	None	3	3	9	Amber	y
4	Loss of IT / hardware failure	Maintenance & recovery contract	2	1	2	Green	N
5	Denial of Access	None	2	3	6	Amber	N

**Business Impact Analysis Matrix**

		Likelihood			
		1	2	3	4
Significance	1		Loss of IT / hardware failure (improved)		Loss of IT / virus (improved)
	2				Loss of IT / virus
	3		Denial of Access	Loss of IT / hardware failure	
	4				

**Key**

	Acceptable. Keep under review
	Room for improvement. Identify and cost risk reduction measures. Decide if implementation is cost effective
	Unacceptable. Identify and implement risk reduction measures

**Risk Analysis Action Log**

Threat No from above	Current Risk Rating	Action Required	Priority	Timescale	Date of Completion	Revised Risk Rating
1	8	Install anti-virus software	Important	3 Months	18/10/200x	4
3	9	Maintenance & Recovery contract	Important	3 months	18/10/200x	2
5	6	No practical measures	N/A	N/A	N/A	6

## Examples of Risk Mitigation and Risk Improvement Measures

The following is a list of suggested risk mitigation / risk improvement measures you may wish to consider. The list is not exhaustive and is in no particular order of priority.

### Computers, Networks and Communications



- Data back up regime including duplicate copies*
- Stand-by power generator provision with “clean” supply via UPS*
- Specific flood protection of computer rooms*
- Safe location of water pipes and services around computer rooms*
- Automatic fire extinguishing system protection for computer room*
- Electrical surge / transient over voltage protection*
- Lightning strike protection*
- Early warning smoke detection in computer rooms (e.g. Vesda)*

*Security protection for hardware*

*Uninterruptible power supply to ensure safe shut down in the event of power failure*

*Data storage regime including off-site storage and storage in fire resisting data cabinets*

### Premises Damage



- Fire sprinkler system*
- Automatic fire alarm installation*
- Scope of automatic fire alarm detection*
- Remote signalling of automatic fire alarm installation*
- Fire extinguisher provision and maintenance*
- Firebreak wall compartmentation*
- Fire stopping of service penetrations in firebreak walls*
- Electrical testing – PAT and fixed wire*
- Enforcement of Smoking regulations*

*Removal of portable heating appliances*

*Kitchen duct cleaning*

*Internal and external housekeeping and control of waste materials*

*“Hot Work Permit” procedures / control of outside contractors*

*Oil tank bunding*

*Burst pipe prevention measures*

*Fire Risk Assessment*

*Arson prevention (by undertaking an arson risk assessment)*

*Construction – use of non combustible or LPCB approved products*

*Boiler rooms / Electric Switch rooms – removal of any storage*

*Careful location of high value fixed equipment e.g. servers to be located 10-15 cms off the ground to reduce their vulnerability to low level flooding*

### Premises Security



- Intruder alarm*
- Intruder alarm scope of detection*
- Intruder alarm remote signalling*
- Intruder alarm key holder response type / level*
- Security safe*
- Security lighting including external areas*
- Perimeter security, e.g. fences, gates, walls, posts*
- CCTV*

*CCTV remote monitoring*

*Security guarding*

*Access control systems*

*Accreditation process for contractors and visitors*

*Secure disposal of sensitive documents*

*Security of portable professional equipment left at the premises and used away from the premises*

*Good quality locks on doors and shutter doors*

*Appropriate level of window security e.g. locks, grilles, bars, shutters*

## **Health and Safety – Employees and others**



*Develop a health and safety policy statement which meets legal duties under the Health and Safety at Work Act 1974 and supports other business exposures e.g. environmental or product quality.*

*Ensure that trained persons are appointed e.g.:*

- *health and safety adviser / competent persons*
- *risk assessors*
- *First Aiders*

*Develop risk assessments to eliminate or control risks e.g.*

- *fire*
- *explosion*
- *ill health arising from potentially hazardous substances*
- *electrocution*
- *pollution*
- *injury / damage attached to product liability*

*Ensure that all employees are provided with health and safety information, instruction and training relevant to their duties.*

*Ensure that trained persons are appointed to e.g.*

- *review and audit risk assessments and other risk control systems*
- *maintain accident / incident records and where necessary carry out investigations*
- *advise and cooperate with relevant enforcing authorities should there be a significant injury, disease or dangerous occurrence.*

## **Business Recovery** [Return to Step 4 Business Recovery Planning](#)



*Sub-contracting (whole or part of activities)*

*Reciprocal agreements*

*Telecomms recovery contract, e.g. BT Commsure*

*Mobile IT recovery contract*

*IT recovery contract with relocation*

*Workplace recovery contract*

*Serviced offices suppliers*

*Short term rent of alternative premises*

*Ability of key staff to work from home*

*Use of other group facilities*

*Serviced offices suppliers / business centres*

*Use of relocatable / portable buildings*

*Use of temporary / agency staff*

## Assistance with Risk Mitigation / Risk Improvement Measures

Please contact the Aviva Risk Management Solutions Risk Helpline on 0845 366 66 66 quoting your Aviva Insurance policy number if you require further guidance on any specific risk mitigation / risk improvement measure. Aviva has negotiated preferred supplier deals for a range of business protection products. These include

- Fire extinguishers
- Safety signage
- Fire cabinets and safety vessels
- Fire data safes and security safes
- Fire safety training
- Security grilles and shutters
- Security posts
- Intruder alarms
- Buildings valuation
- Electrical inspection compliance

Aviva Risk Management Solutions can also provide a range of Health and Safety consultancy and training including Safety Healthcheck, topical seminars and NEBOSH, IOSH and IRM accredited training. Please call 0500 55 99 77 for further details.

## STEP 3 – Emergency Action Planning



The aim is to produce a plan that will enable immediate and effective action to take place should a disaster happen by identifying effective and practical procedure to:

- Assess the extent of the disaster and damage limitation measures.
- Implement short-term recovery arrangements to ensure the minimum acceptable level of service is restored as soon as possible.

The plan should be invoked if minimum service levels are breached or if the Disaster Co-ordinator decides that normal service levels could be impaired for an unacceptable period. Remember what constitutes a disaster will vary from company to company but could constitute:

- Significant damage to premises which would render all or part of it uninhabitable
- Loss of or significant damage to critical equipment which would render it unusable
- Sustained loss of computers or telecommunications due to external factors
- Denial of access to premises

You would expect to find arrangements to cover the following in the final business continuity plan as a result of this process:

- Personnel
- Immediate damage limitation
- Site security
- Damage assessment and salvage
- Invoke contingency arrangements (IT recovery contracts, workplace recovery contracts)
- Maintain an “Emergency Action Log” to record details of their actions, losses identified and expenses incurred
- Communicate with press, stakeholders, suppliers and important customers
- Decide which member of the team will be responsible for which actions

Use [Checklist 1](#) to help you with your emergency action planning.

Finally, ensure that the Disaster Recovery Team has the information and resources they will need to operate successfully in the aftermath of an incident, whether serious or minor. You could prepare an “Emergency Action Box / Toolkit”. This should be located off-site or in a secure place so that it can be accessed quickly after an incident. This ‘box’ should contain items that will assist the team to operate during the initial emergency. We have made a few suggestions, as to what to include, below.

**Note:** You may also wish to append any relevant documents such as emergency evacuation plans and procedures you have prepared to deal with a specific threat such as Terrorism, Bomb Hoax or Suspect Package.

#### **Typical contents of an “Emergency Action Box”**

*A full copy of the Business Continuity Plan*

*Staff lists with contact / cascade details*

*Inventories*

*External contact details*

*Site building plans*

*Location of high value assets / critical & IT equipment to assist the Emergency Services and with salvage operations*

*Electrical cabling routes*

*Electrical switchgear and transformer location*

*Telecommunications and data cabling routes*

*Fire hydrant locations*

*Gas and water mains routes including shut-off valve locations*

*Access points*

*Keys*

*First Aid kit*

*Torches*

*Batteries*

*Writing materials and stationary*

*High visibility jackets and hardhats*

#### **A note on dealing with the media**

Serious incidents may attract attention from the media. The business may be pressed for information about the extent of the situation and its effect on the business, staff, the local environment, employment or any other matters.

Whilst the urgency of recovery from the disaster may be the priority, providing information for the media ensures the company strongly influences the messages that are being reported.

Following a major incident, many customers, employees, suppliers and others will only know what about it through the media. The information they receive may be inaccurate, exaggerated, possibly very negative or simply wrong. It will however, be believed by those that hear it.

Without information from the company the perception may be that control over the situation has been lost and customers etc. may assume the worst.

An inability to communicate with these audiences before, during or after an incident can cause a Public Relations disaster thereby compounding the existing business disaster.

In order to minimise the risk of negative PR and the damage it can do and to enable the organisation to portray itself in a positive and responsible light, a communications plan should form part of any Business Continuity Plan. This might be as simple as:

- Preparing a “holding statement” to deal with initial press enquiries
- Passing media enquiries to your retained solicitor
- Securing the services of a specialist PR company
- Arrange training of a specific senior employee to deal with the media

### **Sample Media Statements**

Until the full extent of the incident is known and the nominated manager to deal with enquiries has arrived, a statement should be given and details taken of the enquirer along the line of the following-

#### **1. Holding Statement**

***"[Insert name] is handling all media enquiries.  
Please can I take your contact details and any specific questions.  
They will get back to you immediately with the information that is available at present."***

Any further information provided by the person in the Disaster Recovery Team dealing with media enquiries should be factual and the person should avoid being drawn by the media into speculating on the “worst case scenario” consequences of the disaster. The implementation of the Business Continuity Plan should be emphasised as a positive measure the business is undertaking to minimise the consequences of the disaster.

In the event of any serious injuries it is essential the business co-operates with the Emergency Services regarding the release of information to avoid any additional stress on the families of those affected.

#### **2. Business Recovery Statement**

If a statement on recovery is required then it should be along the lines of:

***“Our company has experienced a significant disruption to its business at:***

Name and address of the business

***“We are implementing our business recovery plan and everything is being done to provide continued service to our customers at:-***

Temporary Address

***“Normal business activities will be conducted at the above with effect from:***

Planned Recovery Date

***“In the interim, some disruption to our normal service may occur and we would ask for our customers’ understanding during this period.”***

## STEP 4 – Business Recovery Planning

**Business Recovery Planning** - The Disaster Recovery Team should also plan how the business will return to full capacity. This will require the disaster recovery team to think about issues such as:



- Implementing alternative working practices such as working from other Group offices, clients' premises or from home
  - Identifying and equipping temporary premises
  - Monitoring the progress of the reinstatement work at the damaged premises, ensuring that this goes to plan and that office and IT equipment is ordered at the appropriate time
  - Keeping in contact with customers and trying to win back the lost business as capacity improves
- Keeping the "Disaster Recovery Log" up to date by recording details of their actions, losses identified and expenses incurred

Refer to the [Business Recovery](#) examples of Risk Mitigation / Risk Improvement measures above.

Again, [Checklist and Contact List Templates](#) have been supplied with this document.

### Illustration 5 – XYZ Recruitment Consultancy Ltd Recovery Planning

*Minimum Service Level: Update transport engineers in database once a week; update database of vacant positions on a weekly basis; advertise in monthly publications; update vacancies on own website on a weekly basis; arrange interviews within 72 hours of request.*

The risk analysis exercise has identified that in the event of a prolonged denial of access (in excess of 72 hours) the business will fail to meet its minimum service level. It would take 8 weeks to set up offices in alternative premises. However the denial of access is likely to have ended during that 8 week period. Accordingly it will be necessary to continue the business and meet the minimum service level during that period by other means. Such as by -

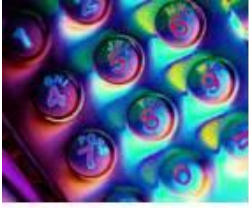
- Acquiring sufficient short term serviced office accommodation (a list of suitable providers and locations is maintained in the contact list section of the Business Continuity Plan)
- Invoking the IT hardware recovery contract and install hardware in above office accommodation
- Requesting website host provider to insert suitable message and update message daily
- Diverting phones to company mobiles and the above office accommodation
- Sending your pre-determined staff to work from home with laptops
- Communicating with customers and agreeing deadline extensions where necessary

The business has decided that the above measures will provide sufficient facilities to enable it to meet its minimum service level.

The planned measures are to be reviewed annually.

**Business Recovery** - The following are examples of business recovery measures.

Telecoms recovery contract, e.g. BT Commsure



- *This would typically involve the provision of a mobile emergency telecoms switching unit*
- *It may be appropriate and cost effective for your business if you have a high dependency on the continued availability of telecoms services*
- *If not your Business Continuity Plan should ensure that suitable alternative communication facilities are made available.*

Mobile IT recovery contract

- *This could typically involve the delivery and installation of alternative servers to your premises to facilitate continuity of your business*
- *Establish if suitable or cost effective for your business*
- *If so, take out contract with a suitable specialist provider*
- *The contract will typically involve a number of test days. These are essential to ensure the IT systems will work in an emergency.*

IT recovery contract with relocation

- *As above but would involve you relocating to the servers at a fixed location e.g. the premises of your service provider*
- *The contract will typically involve a number of test days. These are essential to ensure the IT systems will work in a emergency*
- *If neither IT Recovery action is suitable for your own business then ensure that your IT Disaster Recovery Plan will provide for a full recovery of your core systems within a timescale which is appropriate for you to meet your minimum service standards.*

Workplace recovery contract



- *This is a comprehensive office recovery solution where you can have a contract with a specialist provider for a specified number of workstations, telecoms and IT provision*
- *It can typically be invoked at 4 hours notice*
- *This may be appropriate and cost effective for your business if you have a high dependency on the continued availability of office and associated services – e.g. for a call centre / customer service operation. Establish if this is suitable and cost effective for your business*
- *Again, the contract will typically involve a number of test days. These are essential to ensure the IT systems will work in an emergency.*

Serviced offices / business centres

- *Short term serviced office facilities are available in many areas with specialist suppliers which will allow you to move in within 12 or 24 hours*
- *This may be required until you can find alternative premises. Such premises may be useful for holding meetings with customers and suppliers.*

Short term rent of alternative premises

- *Reinstatement of your current location may be a long drawn out affair so it may be beneficial to move some / all of your activities to an alternative site*
- *Keep in touch with commercial estate agents and landlords to remain aware of what buildings are available within your locality.*

Use of other group facilities



- *If you have other group locations, consider in advance what work / activities can be relocated; try and establish quantities, timescales and other requirements e.g. transport, staffing levels, management required*

- *This may involve a combination of overtime working, relocating staff and hot desking / changing shift patterns*
- *Should it be feasible then consider preparing a detailed Contingency Plan outlining the steps necessary to facilitate this and append to the Business Continuity Plan or keep it available for easy access*

#### Use of relocatable / portable buildings

- *Portable buildings can be delivered to your site quite quickly on the back of a lorry and can be an alternative to obtaining short term serviced accommodation; particularly useful to provide office accommodation, rest room facilities etc*
- *Other semi rigid buildings can be useful to provide training and meeting rooms*
- *Keep a note of contact numbers for these specialist companies*
- *You may wish to consider where such buildings could be located and advance preparations can be made (e.g. level ground, hard-standing, utility connections)*

#### Temporary / agency staff

- *Following a partial loss or move to a temporary site, it may be necessary to hire temporary staff to catch up on orders, recover / reinstate files etc. As with all other recovery measures, make a note of the relevant phone numbers of agencies who can supply you with the required type of staff*

## STEP 5 – Testing and Maintaining the plan

**Testing** - Regular testing of the continuity plan should be carried out to provide assurance that the organisation is adequately protected against any emergency. The objectives being to:-

- ensure that any weaknesses or omissions in the continuity plan are identified
- ensure that any weaknesses or omissions in personnel training and knowledge of the continuity plan are highlighted
- improve the security awareness of personnel
- allow personnel to gain experience of emergency action and recovery procedures
- confirm that the business is serious about the need for continuity planning.



Testing the business continuity plan is a bit like having a fire drill but without the need for everybody to stop work. You could simulate a disaster with a desktop exercise, you could run a full simulation across the whole business or you could run the simulation on different parts of the business at different times.

A desktop exercise would involve the Disaster Recovery Team convening to ask “what if” questions to test how the plan would respond. This is only a discussion amongst the Disaster Recovery Team and the actual business departments are neither involved nor interrogated.

A rehearsal will involve putting your plan into action in a simulated environment. You will involve the actual business departments and external providers of recovery assistance but you may wish to stop short of incurring additional costs. You can rehearse this with the whole business or different parts of the business at different times.

Some businesses engage in a live test where they deliberately shut down or deny access to critical functions within the business, sometimes without warning, to get the most realistic feel for how the business would react in the event of a disaster.

You should document what you learn from these tests and change the provisions of the plan if necessary.

**Maintenance** -The continuity plan should be frequently reviewed and updated. Even small changes to the business can have a big impact on the operation of the plan. Try to incorporate the need to update the plan in as many business change processes such as HR, IT, premises, supply chain and operations management. Lists of contact names should be reviewed quarterly. Other changes that will trigger a review or update of the plan will include -

- deficiencies revealed by actual or test disasters
- changes in staff or circumstances
- new or extended operations
- additional premises
- changing priorities.

After a major change to the plan it will be necessary to test it again.

#### **4 DOCUMENTATION AND COPIES**

Hard copies of the plan should be kept in loose-leaf ring binders to enable additional pages and amendments to be easily incorporated.

Copies of building and site plans should be attached to the plan covering the following details:-

- Electrical cabling routes together with switchgear and transformer location
- Telecommunication and data cabling routes and points of entry into buildings
- Gas and water mains including on and off-site shut-off valve location.
- Access points.
- Emergency equipment location.



Key personnel and their deputies, and all members of the disaster recovery team should hold documented copies of the plan, at home. The Disaster Co-ordinator and deputy should have access to additional copies at each premises. The number of copies held, together with their location, should all be recorded. Updates should be signed for and obsolete sections returned.

#### **5 Further Information and Guidance**

Following a period of consultation, the British Standards Institution published BS 25999-1:2006. This Code of Practice establishes the process, principles and terminology of business continuity management (BCM), providing a basis for understanding, developing and implementing business continuity within an organisation and to provide confidence in business-to-business and business-to-customer dealings. It is intended to serve as a single reference point for identifying ranges of controls for most situations where BCM is practiced no matter what size the organisation or whether it is in the industrial, commercial, public or voluntary sectors.

Part 2, BS 25999-2:2007 was published in late 2007 and specifies the process for achieving certification that the business continuity capability is appropriate to the size and complexity of an organisation.

The links below will provide you with more details on BS 25999 and other business continuity related topics.

#### **Links**

British Standard Institute BSI 25999:  
Department for Business Enterprise  
and Regulatory Reform

[www.bsigroup.co.uk](http://www.bsigroup.co.uk)

UK Resilience:

[www.berr.gov.uk](http://www.berr.gov.uk)

UK Security Service:

[www.ukresilience.info](http://www.ukresilience.info)

Continuity Central

[www.mi5.gov.uk](http://www.mi5.gov.uk)

[www.continuitycentral.com/uk.htm](http://www.continuitycentral.com/uk.htm)

# BUSINESS CONTINUITY PLAN

**Company Name** \_\_\_\_\_

**Issue Date:** \_\_\_\_\_

**Revision Dates:** \_\_\_\_\_

**Test Dates:** \_\_\_\_\_

This plan is designed to assist in the recovery of critical business functions in the event of a disaster. It should not be invoked for minor incidents.

## CONFIDENTIAL – RESTRICTED ACCESS

Numbered copies of this plan should be held by the members of the Disaster Recovery Team and held securely by them off-site. All names, addresses and contact numbers listed in this plan are for emergency use only and are confidential to the holders of the plan.

**Copy** \_\_\_\_\_ **of** \_\_\_\_\_

## Related Documents / Plans

Document Title	Document owner	Attached to plan Y/N

**DISASTER RECOVERY TEAM**

**FORM A**

[Return to Disaster Recovery Team](#) [Return to Step 1 – Service Levels](#)

<b>Position / Role</b>	<b>Name</b>	<b>Home Address</b>	<b>Home Telephone No.</b>	<b>Mobile No.</b>
<i>Disaster Co-ordinator</i>				
<i>Deputy Disaster Co-ordinator</i>				
<i>Disaster Recovery Team Member 1</i>				
<i>Deputy Team Member 1</i>				
<i>Disaster Recovery Team Member 2</i>				
<i>Deputy Team Member 2</i>				
<i>Disaster Recovery Team Member 3</i>				
<i>Deputy Team Member 3</i>				
<i>Disaster Recovery Team Member 4</i>				
<i>Deputy Team Member 4</i>				

The Deputy Disaster Co-ordinator is a permanent member of the Team. Other deputies should be called upon only if the original team member is unavailable, e.g. illness or holiday. Deputies will be required to keep a copy of the Business Continuity Plan

The initial meeting to be held at	
Or, if unavailable at Adequate telephone and fax lines and mobile phones should be available	

## **Core Business Objectives Statement**

*Copy the statement from Step 1- Service Levels*

Return to this statement if you need to re-focus on the primary business objectives to avoid consideration of issues that do not impinge directly on the protection and the survival of your business. You can return to this statement at any time during the planning process or if you have invoked the plan.

## **SERVICE LEVELS LOG AND PLAN INVOCATION PROCEDURES**

**FORM B**

[Return to Introduction](#) [Return to Step 1- Service Levels](#)

### **Statement of normal service levels**

*Copy the statement from Step 1- Service Levels here*

### **Statement of minimum service levels**

*Copy the statement from Step 1- Service Levels here*

**The objective of the Business Continuity Plan is to ensure the business restores minimum service levels following any incident and returns to normal service levels as quickly as possible. (amend if necessary e.g. to include timescales)**

**The plan should be invoked if minimum service levels are breached or if the Disaster Co-ordinator (or deputy) decides that normal service levels could be impaired for an unacceptable period. (amend if necessary e.g. to include timescales)**

**This plan does not encompass a catastrophic event which makes the majority of the staff unavailable in addition to the physical premises and assets of the business. Also, this document should not be invoked for minor incidents.**

**SERVICE LEVELS – DEPARTMENTAL QUESTIONNAIRE TEMPLATE**

**FORM C**

[Return to Step 2-Risk Analysis](#)

<b>To:</b>		<b>From:</b>		<b>Reply by:</b>	
------------	--	--------------	--	------------------	--

**Action:** Read the statement of minimum service levels below. This is the level of service that our business must continue to provide in the event of a disaster. Use the form below to specify what processes your department / function has to provide to support this, what resources / assets / staff are required for this and what timescales are involved in providing this service. Some of the information may already be recorded in individual departmental contingency plans e.g. IT. Expand the table if required

**Statement of minimum service levels**

*Copy the statement from Step 1- Service Levels here*

	<b>Process</b>	<b>Resource / Asset required</b>	<b>Timescale to provide</b>
1			
2			
3			
4			
5			
6			

**CRITICAL BUSINESS PROCESS LOG**[Return to Step 2-Risk Analysis](#)[Return to Risk Rating Method](#)**FORM D**

	<b>Critical Business Process</b>	<b>Person with Operational Responsibility</b>	<b>Assigned Disaster Recovery Team Member</b>
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			

**RISK ANALYSIS FORM**

**FORM E**

[Return to Step 2-Risk Analysis](#)

	<b>Threat</b>	<b>Mitigation Measure</b>	<b>Likelihood (A)</b>	<b>Significance (B)</b>	<b>Risk Rating (A x B)</b>	<b>Red / Amber / Green</b>	<b>Action (Y / N)</b>
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

**BUSINESS IMPACT ANALYSIS MATRIX**

[Return to Risk Rating Method](#)

**FORM F**

		Likelihood			
		1	2	3	4
Significance	1				
	2				
	3				
	4				

Key	
	Acceptable. Keep under review
	Room for improvement. Identify and cost risk reduction measures. Decide if implementation is cost effective
	Unacceptable. Identify and implement risk reduction measures

**RISK ANALYSIS ACTION LOG**

**FORM G**

[Return to Risk Rating Method](#)

Threat No from above	Current Risk Rating	Action Required	Priority	Timescale	Date of Completion	Revised Risk Rating

## CHECKLISTS AND CONTACT LISTS

[Return to Business Recovery Planning](#)

Checklist No. 1	<b>Emergency Action Checklist</b>
Checklist No. 2	<b>Business Recovery Checklist</b>
Checklist No. 3	<b>Business Continuity Plan Maintenance Record</b>
Checklist No. 4	<b>Business Continuity Plan Test Record</b>
Checklist No. 5	<b>Emergency Action Log</b>
Checklist No. 6	<b>Business Recovery Log</b>

Contact List No. 1	<b>Computer Equipment Suppliers</b>
Contact List No. 2	<b>Telecommunication Equipment Suppliers</b>
Contact List No. 3	<b>Insurance</b>
Contact List No. 4	<b>Specialist Salvage Companies</b>
Contact List No. 5	<b>Office Furniture and Equipment Suppliers</b>
Contact List No. 6	<b>Transport Firms</b>
Contact List No. 7	<b>Building Firms</b>
Contact List No. 8	<b>Utility Suppliers</b>
Contact List No. 9	<b>Electricians, Plumbers, Registered Gas Fitters and Facilities Engineers</b>
Contact List No. 10	<b>Building Services Suppliers</b>
Contact List No. 11	<b>Estate Agents, Land Agents and Landlords</b>
Contact List No. 12	<b>Planning Authority, Licensing Authorities, Regulatory Authorities and Trade Bodies</b>
Contact List No.13	<b>Staff</b>
Contact List No.14	<b>Major Clients</b>
Contact List No.15	<b>Media Contacts</b>

**CHECKLIST NO. 1 - EMERGENCY ACTION CHECKLIST**

[Return to Step 3-Emergency Action Planning](#)

You can amend this checklist to meet your own requirements

		Assigned to	Start Date/Time	Completion Date/Time
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				

		Assigned to	Start Date/Time	Completion Date/Time
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				

**CHECKLIST NO. 1 - EMERGENCY ACTION CHECKLIST (Continued)**

**EMERGENCY ACTION PLANING**

## CHECKLIST NO. 2 - BUSINESS RECOVERY CHECKLIST

You can amend this checklist to meet your own requirements

		Assigned to	Start Date/Time	Completion Date/Time
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				

		Assigned to	Start Date/Time	Completion Date/Time
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				

**CHECKLIST NO. 2 – BUSINESS RECOVERY CHECKLIST (Continued)**

**BUSINESS RECOVERY PLANING**

**CHECKLIST NO.3 – BUSINESS CONTINUITY PLAN MAINTENANCE RECORD**

<b>Full Plan Review / Appendices Only:</b>		<b>Business Department:</b>	
<b>Completed By:</b>		<b>Date:</b>	

<b>Detailed Findings</b>	<b>Recommendations / Amendments</b>	<b>Actioned By</b>	<b>Completion Date</b>

Note: Retain any relevant papers with this record

**CHECKLIST NO.4 – BUSINESS CONTINUITY PLAN TEST RECORD**

<b>Type of Test:</b>		<b>Business Department:</b>	
<b>Completed By:</b>		<b>Date:</b>	

<b>Detailed Findings</b>	<b>Recommendations / Amendments</b>	<b>Actioned By</b>	<b>Completion Date</b>

Note: Retain any relevant papers with this record

**CHECKLIST NO. 5 – EMERGENCY ACTION LOG**

<b>Date / Time</b>	<b>Action / Decision / Information Record</b>	<b>Logged by</b>



**CHECKLIST NO. 6 – BUSINESS RECOVERY LOG**

<b>Date / Time</b>	<b>Action / Decision / Information Record</b>	<b>Logged by</b>



**CONTACT LIST NO. 1 - COMPUTER EQUIPMENT SUPPLIERS**

	<b>Equipment Model No. /Serial No.</b>	<b>Delivery Period</b>	<b>Manufacturer/Supplier/ Contact Name</b>	<b>Telephone Nos. (including out of hours)</b>	<b>E-mail / web address / fax</b>	<b>Mobile No.</b>
1						
2						
3						
4						
5						
6						
7						
8						

**CONTACT LIST NO. 2 - TELECOMMUNICATION EQUIPMENT SUPPLIERS**

	<b>Equipment Model No. /Serial No.</b>	<b>Delivery Period</b>	<b>Manufacturer/Supplier/ Contact Name</b>	<b>Telephone Nos. (including out of hours)</b>	<b>E-mail / web address / fax</b>	<b>Mobile No.</b>
1						
2						
3						
4						
5						
6						
7						
8						

**CONTACT LIST NO. 3 - INSURANCE**

		<b>Address</b>	<b>Telephone Nos. (including out of hours)</b>	<b>E-mail / web address / fax</b>	<b>Mobile No.</b>
1	Insurance Intermediary				
2	Loss Adjuster				
3	Insurance Company				

**CONTACT LIST NO. 4 - SPECIALIST SALVAGE COMPANIES INCLUDING THOSE DEALING WITH RECOMMISSIONING OF ELECTRONIC HARDWARE, SALVAGE OF MAGNETIC MEDIA, DOCUMENTATION AND OTHER RECORDS**

	<b>Name</b>	<b>Address</b>	<b>Telephone Nos. (including out of hours)</b>	<b>E-mail / web address / fax</b>	<b>Mobile No.</b>
1					
2					
3					
4					
5					
6					

**CONTACT LIST NO. 5 - OFFICE FURNITURE and EQUIPMENT SUPPLIERS**

	<b>Name</b>	<b>Address</b>	<b>Telephone Nos. (including out of hours)</b>	<b>E-mail / web address / fax</b>	<b>Mobile No.</b>
1					
2					
3					
4					
5					
6					

**CONTACT LIST NO. 6 - TRANSPORT FIRMS**

	<b>Name</b>	<b>Address</b>	<b>Telephone Nos. (including out of hours)</b>	<b>E-mail / web address / fax</b>	<b>Mobile No.</b>
1					
2					
3					
4					
5					
6					

**CONTACT LIST NO. 7 - BUILDING FIRMS**

	<b>Name</b>	<b>Address</b>	<b>Telephone Nos. (including out of hours)</b>	<b>E-mail / web address / fax</b>	<b>Mobile No.</b>
1					
2					
3					
4					
5					
6					

**CONTACT LIST NO. 8 – UTILITY SUPPLIERS**

	<b>Name</b>	<b>Address</b>	<b>Telephone/ Fax Nos. including out of hours)</b>	<b>Email / web site Nos.</b>	<b>Mobile No.</b>
1	National Grid - Gas (UK gas transportation and emergency service)				
2	Regional Electricity Distribution Network Operator	<i>A map where you can check who your regional electricity Distribution Network Operator is can be found at -</i> <a href="http://www.nationalgrid.com/uk/Electricity/AboutElectricity/DistributionCompanies/">http://www.nationalgrid.com/uk/Electricity/AboutElectricity/DistributionCompanies/</a>			
3					
4					
5					
6					

**CONTACT LIST NO. 9 – ELECTRICIANS, PLUMBERS, REGISTERED GAS FITTERS AND FACILITIES ENGINEERS**

	<b>Name</b>	<b>Address</b>	<b>Telephone Nos. (including out of hours)</b>	<b>E-mail / web address / fax</b>	<b>Mobile No.</b>
1					
2					
3					
4					
5					
6					

**CONTACT LIST NO. 10 – BUILDING SERVICES SUPPLIERS**

	<b>Name</b>	<b>Address</b>	<b>Telephone Nos. (including out of hours)</b>	<b>E-mail / web address / fax</b>	<b>Mobile No.</b>
1					
2					
3					
4					
5					
6					
7					
8					

**CONTACT LIST NO. 11 - ESTATE AGENTS, LAND AGENTS AND LANDLORDS**

	<b>Name</b>	<b>Address</b>	<b>Telephone Nos. (including out of hours)</b>	<b>E-mail / web address / fax</b>	<b>Mobile No.</b>
1					
2					
3					
4					
5					
6					

**CONTACT LIST NO. 12 – PLANNING AUTHORITY, LICENSING AUTHORITIES, REGULATORY AUTHORITIES AND TRADE BODIES**

	<b>Name</b>	<b>Address</b>	<b>Telephone Nos. (including out of hours)</b>	<b>E-mail / web address / fax</b>	<b>Mobile No.</b>
1					
2					
3					
4					
5					
6					
7					
8					

**CONTACT LIST NO. 13 - STAFF**

	<b>Name</b>	<b>Address</b>	<b>Telephone Nos. Mobile No.</b>	<b>e-mail</b>	<b>Key holder Y/N</b>
1					
2					
3					
4					
5					
6					
7					

**CONTACT LIST NO. 13 - STAFF**

	<b>Name</b>	<b>Address</b>	<b>Telephone Nos. Mobile No.</b>	<b>e-mail</b>	<b>Key holder Y / N</b>
8					
9					
10					
11					
12					
13					
14					

**CONTACT LIST NO. 13 - STAFF**

	<b>Name</b>	<b>Address</b>	<b>Telephone Nos. Mobile No.</b>	<b>e-mail</b>	<b>Key holder Y / N</b>
15					
16					
17					
18					
19					
20					
21					

**CONTACT LIST NO. 13 - STAFF**

	<b>Name</b>	<b>Address</b>	<b>Telephone Nos. Mobile No.</b>	<b>e-mail</b>	<b>Key holder Y / N</b>
22					
23					
24					
25					
26					
27					
28					

**CONTACT LIST NO. 13 - STAFF**

	<b>Name</b>	<b>Address</b>	<b>Telephone Nos. Mobile No.</b>	<b>e-mail</b>	<b>Key holder Y / N</b>
29					
30					
31					
32					
33					
34					
35					

**CONTACT LIST NO. 13 - STAFF**

	<b>Name</b>	<b>Address</b>	<b>Telephone Nos. Mobile No.</b>	<b>e-mail</b>	<b>Key holder Y / N</b>
36					
37					
38					
39					
40					
41					
42					

**CONTACT LIST NO. 13 - STAFF**

	<b>Name</b>	<b>Address</b>	<b>Telephone Nos. Mobile No.</b>	<b>e-mail</b>	<b>Key holder Y / N</b>
43					
44					
45					
46					
47					
48					
49					

**CONTACT LIST NO. 13 - STAFF**

	<b>Name</b>	<b>Address</b>	<b>Telephone Nos. Mobile No.</b>	<b>e-mail</b>	<b>Key holder Y / N</b>
51					
52					
53					
54					
55					
56					
57					

**CONTACT LIST NO. 13 - STAFF**

	<b>Name</b>	<b>Address</b>	<b>Telephone Nos. Mobile No.</b>	<b>e-mail</b>	<b>Key holder Y / N</b>
58					
59					
61					
62					
63					
64					
65					

**CONTACT LIST NO. 14 - MAJOR CLIENTS**

		<b>Address</b>	<b>Telephone Nos. (including out of hours)</b>	<b>E-mail / web address / fax</b>	<b>Mobile No.</b>
1					
2					
3					
4					
5					
6					

**CONTACT LIST NO. 14 - MAJOR CLIENTS**

		<b>Address</b>	<b>Telephone Nos. (including out of hours)</b>	<b>E-mail / web address / fax</b>	<b>Mobile No.</b>
7					
8					
9					
10					
11					
12					

**CONTACT LIST NO. 15 – MEDIA CONTACTS**

	<b>Name</b>	<b>Address</b>	<b>Telephone Nos. (including out of hours)</b>	<b>E-mail / web address / fax</b>	<b>Mobile No.</b>