

# **Business Continuity Plan Template and Guidance**

## **Disclaimer**

This guide and template has been produced to provide general information and advice about developing Business Continuity Plans for small to medium sized businesses or voluntary sector organisations. It is not intended to provide detailed or specific advice to individuals or their businesses. If required you should seek professional advice to help develop an individual plan for your business. Sutton Council will accept no liability arising from the use of this document.

## **Aim**

This document has been produced to assist businesses mitigate and prepare for incidents which may affect operations. Once completed, the document should be shared with applicable members of staff who will act as the Incident Management Team (IMT).

The aim of the plan is to provide a reference tool for the actions required during or immediately following an emergency or incident that threatens to disrupt normal business activities. The plan will assist the continuation of business critical activities by minimising the impact of any damage to staff, premises, equipment or records.

## **Process**

Follow these three simple steps:

- Step 1 – Identify your key products / services / activities. Identify which ones are the most important to the organisation and your stakeholders, based on a High, Medium and Low basis.
- Step 2 – Identify the risks that could prevent or interrupt your business from operating normally. At this stage, it is a good idea to try and identify ways of protecting your business from these known risks.
- Step 3 – Produce a Business Continuity Plan for your organisation.

## **Insurance**

As part of the review process for Business Continuity Management; consider whether the insurance you have in place is sufficient to help your business recover, should the worse happen. From the risks identified to your business, what does your policy cover? Include details of your insurer / broker in the plan.

In addition, consider business interruption and cyber insurance policies as applicable to your business.

The ability to demonstrate that you are actively managing and reducing risks may be beneficial when discussing premiums with your insurer; you may be able to negotiate a better deal.

### Step 1 - Key products / services / activities

- List **all** the activities within your business with a brief description of what the activities do, how they are resourced, and how they are prioritised ('High' referring to the activity as critical and 'Low' referring to non-critical activities).

Product / Activity	Brief Description	Resources	Priority Level
<i>EXAMPLE: Receiving orders for products or services</i>	<i>EXAMPLE: Answering telephone or email with orders or enquiries from customers.</i>	<i>Phone line, access to network, staff, office facility, power, information / data.</i>	<i>High</i>

### Step 2 – Identify Risks (Examples shown)

Impact	Possible Risk	Possible Mitigation / Treatment	Business Recovery Strategy
Loss of buildings, work environment and associated utilities	<i>Fire</i>	<i>Monitored fire alarm, firefighting equipment, trained fire marshals.</i>	<i>Work from alternative location and claim insurance.</i>
	<i>Flood</i>		
	<i>Blocked access- cordons</i>		
	<i>Power failure</i>		
	<i>No water</i>		
Loss of staff	<i>Severe weather</i>	<i>Receiving 'Weather Warnings' triggering communication with staff, customers and suppliers.</i>	<i>Work from home; ensure enough local staff can continue highest priority work.</i>
	<i>Pandemic or other communicable disease</i>		

Impact	Possible Risk	Possible Mitigation / Treatment	Business Recovery Strategy
	<i>Transport strike</i>		
	<i>Industrial action</i>		
	<i>Loss of key person / knowledge</i>		
Loss of information / data	<i>IT network failure</i>		
	<i>Loss of portable device (i.e. laptop)</i>	<i>Data encryption and password protecting all portable devices</i>	
	<i>Fire damage to paper records</i>		
Loss of IT Systems	<i>Server failure</i>		
	<i>Cyber attack</i>	<i>Anti-virus software kept up to date.</i>	<i>Safely backing up data.</i>
	<i>Computer failure</i>		
Loss of partner / supplier / contractor	<i>Company enters receivership</i>		
	<i>Incident affecting supplier organisation</i>		

# Business Continuity Plan for [Insert name of organisation]

## Version Control

Author	Version	Date	Review Date	Notes
<i>J. Bloggs</i>	<i>1.0</i>	<i>May 2017</i>	<i>May 2018</i>	<i>First draft</i>

## Distribution list- Employees, stakeholders and partners

Name	Role	Dept. / Organisation

## Contents

1. Introduction .....	3
1.1. Purpose and Scope .....	3
2. Critical Activities.....	3
3. Incident Management .....	4
3.1. Incident Definition .....	4
3.2. Establish the situation.....	4
3.3. Invoking the Plan .....	4
3.4. Incident Response .....	5
3.4.1. Immediate Response Checklist .....	5
3.4.2. Ongoing Response Checklist .....	6
3.5. Standing the Plan Down .....	7
Appendix 1. Incident Management Team (“IMT”) members.....	8
Appendix 2. Other staff Contact Details .....	8
Appendix 3. External contacts .....	9
Appendix 4. Utilities .....	10
Appendix 5. Damage Assessment .....	10
Appendix 6. Salvage.....	11
Appendix 7. Activity / Expenditure Log.....	12

## 1. Introduction

### 1.1. Purpose and scope

The purpose of this Business Continuity Plan is to enable the operations of [insert name of organisation] to survive an incident that disrupts normal operations and working practices.

The responsibility for the maintenance of the plan lies with [Insert name or role].

The responsibility for the initial response lies with [insert name or role], who will work with the selected members of the organisation to form the Incident Management Team (“IMT”).

The plan will include an adequate level of detail used to maintain the business and:

- To ensure a prepared approach to an emergency/incident.
- To facilitate an organised and co-ordinated response to an emergency/incident.
- To provide an agreed framework within which people can work in a concerted manner to solve problems caused by an emergency/incident.

The plan will also help to identify actions that could be taken in advance of an emergency or incident to reduce the risk of it happening.

The plan has been written to reduce the potential impact of an incident by being prepared to maintain services in the event of the:

- Loss of key premises
- Loss of key staff
- Loss of IT / data
- Loss of telecommunications
- Loss of hard data / paper records
- Loss of utilities (electricity, water, gas)
- Loss of a key partner or supplier
- Disruption due to industrial action
- Disruption due to severe weather

## 2. Critical Activities

Whilst most parts of any business are considered important, if an incident did occur, priority must be given to the restoration of the activities that are deemed to be business critical to the performance of the company.

The main critical activities for the organisation are:

- I. [Insert activity name. Description]
- II. [Insert activity name. Description]
- III. [Insert activity name. Description]

These individual activities must be given preferential access to premises, staff, equipment or records if an emergency situation restricted their overall availability. It is for these activities that plans need to be prepared.

### 3. Incident Management

#### 3.1. Incident definition

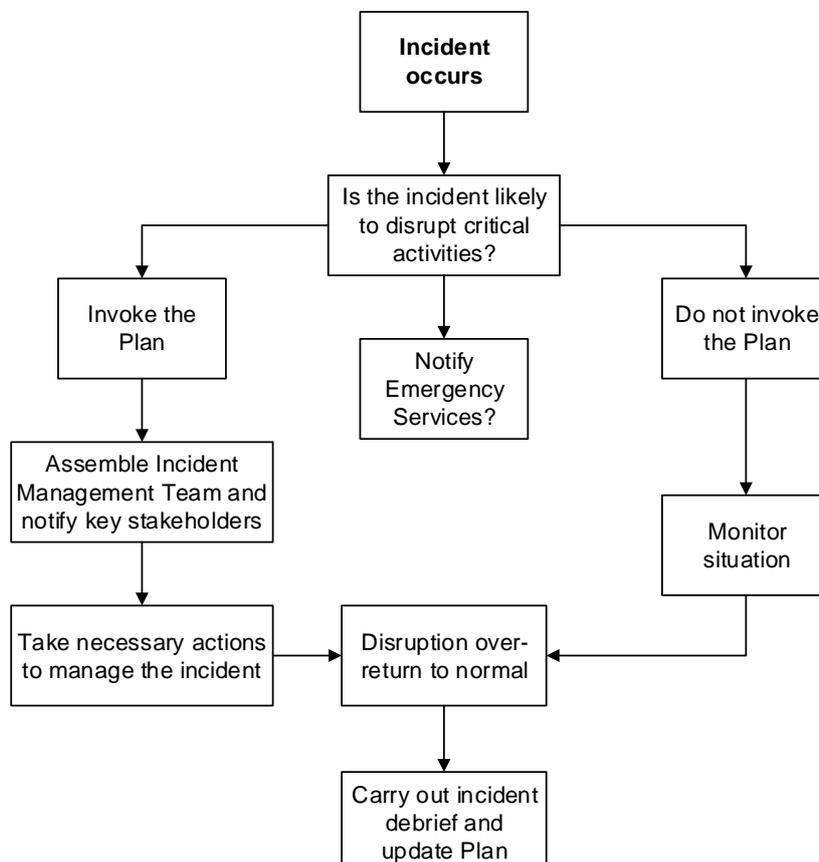
An incident may be any situation which might or could lead to a disruption, loss, emergency or crisis affecting the normal operations of the organisation. Incident Management Team (IMT) members should bear in mind that a minor emergency may have the potential to worsen and escalate.

#### 3.2. Establish the situation

- What has happened? How potentially serious is it?
- When and where did it occur?
- Have the Emergency Services been notified (if applicable)?
- Who else has been informed?
- Is there access to the site?
- Are the IT systems and services still running?
- Are there any casualties? If so, details?
- What actions need to be taken to reduce the impact on the organisation?
- Who needs to be involved in the response?
- What actions should the organisation take at this time, based on the current facts?
- Who is maintaining a record of actions / decisions?
- If the decision is to relocate staff, where will they relocate to?

#### 3.3. Invoking the plan

The IMT will assess the nature and extent of a disruptive incident and its potential impact on the services, taking into consideration the decision whether to invoke the plan or not.



### 3.4. Incident response

#### 3.4.1. Immediate response checklist

Action	Notes	Completed
If necessary: <ul style="list-style-type: none"><li>Follow evacuation procedures</li><li>Call emergency services</li></ul>		
Ensure safety and welfare of all affected persons.		
Call a meeting of the Incident Management Team (Appendix 1). The IMT will coordinate the actions and manage communications.		
Commence a log of all emergency actions taken.		
Assess the situation and level of response required. Can it be dealt with as a day-to-day management issue or does the plan need to be invoked?		
Communications: <ul style="list-style-type: none"><li>Advise staff of the immediate implications for them and service provision</li><li>Advise staff of the immediate requirements to deal with the situation, including temporary accommodation etc if required.</li><li>If necessary, advise key partners / suppliers.</li><li>If necessary speak to the local press.</li></ul>		
If necessary, allow all staff to contact home to advise they are safe.		
If necessary arrange for the premises to be secured.		
If necessary, use signage to advise the move to a temporary location.		
[Add additional actions as required.]		

### 3.4.2. Ongoing response checklist

Action	Notes	Completed
Once you are in control of the initial emergency update staff on a regular basis and keep them fully informed of developments. Make sure members of staff not directly involved in the incident, or those who are absent are also kept advised of developments.		
Priority should be given to the needs of the business critical activities (see Section 2).		
Advise all staff and key contacts of temporary location & any temporary telephone numbers to be used until numbers can be diverted.		
If mobile phones are being used make sure there are sufficient chargers available.		
IT team start sourcing replacement IT equipment, if required.		
Temporary accommodation <ul style="list-style-type: none"> <li>Is the available accommodation sufficient for the needs of all the business critical activities or is additional alternative space required?</li> <li>Do you need to arrange for replacement equipment to be ordered?</li> <li>Do you have access to all essential systems or records?</li> <li>Make arrangements for telephones and post to be re-directed to your new location.</li> </ul>		
Working at home and non-business critical staff <ul style="list-style-type: none"> <li>If available space is at a premium consider allowing suitable individuals to work from home</li> <li>Non-essential staff should be sent home or reallocated to support business critical activities.</li> <li>Make sure those sent home are aware of when to make contact to check on progress or when to return to work.</li> </ul>		
Messages for the media, staff, clients, suppliers and other stakeholders are formulated and cascaded.		
Temporary staff sourced, if applicable.		
Create any new / temporary operational procedures and instructions.		
Closely monitor staff issues, morale, overtime, welfare, etc. Do any of the staff need counselling?		
Do you need to complete an Accident Log?		

Action	Notes	Completed
When ready, inform other organisations, public, suppliers, etc of resumption of normal service / contact details.		
Financial procedures <ul style="list-style-type: none"> <li>Decide who can authorise additional expenditure</li> <li>Keep records of all expenditure</li> <li>Urgent electronic payments managed from home or at the bank branch</li> </ul>		
Inform insurers of a potential claim.		
Cancel or delegate any unnecessary meetings not connected to the incident		
Preservation of records <ul style="list-style-type: none"> <li>Do not destroy anything. Try to recover as many documents as possible and preserve them somewhere where they can be retrieved easily. This is an ongoing obligation throughout and after the incident.</li> <li>Make someone responsible for co-ordinating and preserving a Master Activity Log.</li> <li>Make a record of all meetings and briefing sessions.</li> <li>Make a hard copy of any relevant computer data and electronic mail.</li> </ul>		
Support the post-incident evaluation by direct contribution and by facilitating the involvement of key members of staff. Recovery should always be treated as an opportunity to improve the business.		
Conduct a post incident debrief: <ul style="list-style-type: none"> <li>What worked well?</li> <li>What didn't work so well?</li> <li>What changes need to be made for the future?</li> </ul>		
Review the Business Continuity Plan to learn from the decisions taken.		
Add additional actions as required.		

### 3.5. Standing the plan down

The plan is either stood down when:

- the affected site has been restored to full operational capacity or a new site has been sourced, equipped and is able to handle normal operations,
- data is secured and recovered,
- operations have been restored to pre-incident levels,
- staffing issues have been resolved and all departments have sufficient personnel to undertake their critical activities.

The decision to stand the plan down is taken by the IMT.

**Appendix 1. Incident Management Team (“IMT”) members**

Name	Job Title	Mobile Number	Office Number	Home Number

**Appendix 2. Other staff contact details**

Name	Job Title	Mobile Number	Office Number	Home Number

Include the names and contact numbers of all relevant staff. If an incident occurs (during or outside work hours) you need to be able to inform them, and they may need to take necessary action. Remember to keep this section up to date, detailing when staff leave and join the organisation.

**Appendix 3. External contacts**

Organisation	Contact Name	Main Office N°	Alternative N°
Electricity			
Gas			
Telecommunications			
Water			
Ambulance	Emergencies	999	
Fire Service	Emergencies	999	
Flood line	Information service	0845 988 1188	
Police	Emergencies	999	
Local Hospital			
Sutton Council		020 8770 5000	
Insurer / Broker			
Bank			
[Add Suppliers]			

**Appendix 4. Utilities**

<b>Utility</b>	<b>Location &amp; Operational Details</b>	<b>Responsible Person</b>
Gas Supply Valve		
Electricity Mains Switch		
Water Cut-Off Valve		

**Appendix 5. Damage assessment**

<b>Area Affected</b>	<b>Structure Damage</b>	<b>Office Equipment</b>	<b>ICT Affected</b>	<b>Other</b>

Ensure suitably qualified personnel with appropriate Personal Protective Equipment (PPE) are allocated to carry out damage assessment duties. Approval to enter the premises must be sought from the Emergency Services, where applicable.

**Appendix 6. Salvage**

Department	Items Required	Location	Notes	Priority
EXAMPLE: Finance	Card Reader	Finance Office Cupboard	N/A	High

Ensure suitably qualified personnel with appropriate PPE are allocated to carry out salvage duties.

**Appendix 7. Activity / expenditure log**

<b>Date / Time of Action</b>	<b>Action Taken</b>	<b>Expenditure</b>	<b>Authorised By</b>