Business Continuity

About the Local Resilience Forum

The Hampshire and Isle of Wight Local Resilience Forum comprises of local Emergency Service Responders (Police, Fire, Ambulance), Local Authorities, as well as associated businesses, organisations and voluntary sector representatives that come under the Civil Contingences Act 2004.

Through the Local Resilience Forum, these organisations work together to prepare for, respond to, and recover from emergencies.

Further information on the activities of the Local Resilience Forum can be found online at www.hampshireprepared.co.uk or www.iowprepared.co.uk or by using the contact details at the back of this booklet.

Business Continuity

Brought to you by your Local Resilience Forum

"Business Continuity is an holistic management process that identifies potential business impacts that threaten an organisation and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities"

Business Continuity Institute

If you or your business are involved in an incident and believe you may be in danger always dial 999 and request the appropriate emergency assistance.

If you are not in danger but may be affected indirectly, you may be advised to **GO IN, STAY IN, TUNE IN.**

WHAT IS BUSINESS CONTINUITY?

Business Continuity provides a framework for building organisational resilience with the capability for an effective response that safeguards the your interests, the interests of key stakeholders, reputation, brand and value-creating activities.

Business Continuity is not only having plans written down, it is about understanding your business and empowering your staff to react effectively to any challenges.

The way in which you plan for and respond to such events as fire, flooding, vandalism, loss of utilities, will determine how quickly and to what level your business can recover.

Think about the following key areas:

- Premises
- People
- Communications
- Equipment / stock
- Computers, network access and telecoms
- Financial issues
- Sources of help and advice

Business Continuity does not need to be a complicated process with lots of technical language. It is a common sense approach – writing down useful information in case of an incident big or small!

Why does my business need a plan?

A Business Continuity Plan (BCP) containing all the information you need during and following an incident (such as contact details and action cards) will help you to respond and recover more effectively and efficiently.

It is important that you can respond effectively to be able to support your customers, your brand, reputation and key activities.

It does not matter how big or small your business is, having a plan is the most effective way to navigate any hurdles or incidents you may face.

A Business Continuity Plan allows you to identify what your critical activities are for your business, what threats your business might face, and identify some mitigation strategies in case something does go wrong.

General Considerations	Yes	No	Don't know
Has the idea of Business Continuity Management (BCM) been approved by the owner/partners/board?			
Do you have a Business Continuity Plan (BCP)?			
Is the plan documented clearly and easily accessible?			
Have you exercised your plan within the last 12 months?			
Do you have a policy for how and when to activate your plan?			
Do you regularly review and update your plan?			
Are your staff trained in activating and operating your plan?			
Is there someone in your organisation who will have responsibility for looking after Business Continuity?			
Have you made a list of all key contacts' telephone numbers?			
Have you prepared an emergency pack?			

How do I start?

1) Get to grips with your business:
- What is the aim of your business and what are the key activities involved in achieving it?
- What resources do the key activities need to be able to happen? Think about staff, premises, equipment, communication links, IT, suppliers, specific knowledge or training.
- What deadlines do you work to?

2) Assess the Risk
- What risks does your business face?
- What critical activities might be impacted?

3) Develop a strategy:
- What actions will you take in a crisis
- How the actions will be done
- Who will do those actions
- Where the actions will take place. For example, on-site or at an alternative location
- What the priorities will be.

4) Write your plan:
- Use the information you have gathered to write the plan
- There is some guidance in this booklet, or template available from the resources detailed later

5) Test your plan
- You should test your plan to make sure that your assumptions work.
- Staff must become familiar with it and have an idea of what would happen in a real incident.
- Use some of the scenarios in this booklet to help you get started

6) Maintain your plan
- Review your plan on a regular cycle
- An out of date plan could be almost useless when you actually need to use it

What does my Business Continuity Plan need to contain?

- ✓ Introduction
- ✓ Aims & objectives
- ✓ Key critical business activities list, with their critical time frames (how long can you cope before getting this activity started again)
- ✓ Known potential risks & threats
- ✓ Plan triggers
- ✓ Activation process
- ✓ Action cards for response
- ✓ Recovery process
- ✓ Key contacts, customers, suppliers, staff, other stakeholders

How do I get advice to write a plan?

There are a number of different sources of advise and templates;

- The government business continuity toolkit
- The Business Continuity Institute (BCI)
- BCI Good Practice Guidelines – a step by step guidance document
- Your Local Resilience Forum
- Template available online

Links are available at the end of the booklet

Checklist of things to consider for a Business Continuity Plan

These are not exhaustive lists but questions to prompt your planning process.

If you answer yes, make sure you capture those details in your plan.

If you answer no or don't know, consider if these are relevant to your business, and if they are find out more to include in your plan.

Equipment and Documents	Yes	No	Don't know
Have you identified your key equipment?			
Do you have contingency plans in place to cater for the loss/ failure of key equipment?			
Do you regularly update an inventory of your company equipment?			
Do you have controls over the movements of your company equipment?			
Do you regularly copy/backup your information?			
Are your critical documents adequately protected?			
Do you have copies of your critical records at a separate location?			

Buildings and people	Yes	No	Don't know
Do you have emergency evacuation procedures for your building?			
Do you have access to your building at all times?			
Do you have fire safety procedures in place?			
Do you have access to an alternative workspace to use in an emergency?			
Have you got a list of all employee contact telephone numbers and home addresses? Where is this stored?			
Have your staff been given specific roles in the event of a crisis?			
If your business could not operate from its present location could your staff work from an alternative location, or some of them work from home etc?			
Do you have members of staff with first aid or medical training?			
Have you identified and considered the risks from your surrounding area and businesses? E.g. Flood risk,			

IT	Yes	No	Don't know
Are your IT systems critical to the running of your business?			
If your IT systems went down do you have manual processes that could maintain critical documentary/administrative functions?			
Do you know how long it would take to recover IT functions if your system went down?			
Who would restore your system if it went down and do you have their contact details?			
Do you have a tested IT disaster recovery plan?			
Is your computer anti-virus software up to date?			
Are documented IT security policies and procedures in place?			
re all your computer users fully aware of email and internet usage policies?			
Is your company system part of a larger network?			
Do you know how many platforms/servers/applications or operating systems support critical business functions?			
Is expertise of how to use your IT system, knowledge of where critical documents are electronically stored etc, limited to one individual?			
Do you have vital computer information stored on back up discs held off premises?			

Customers and Suppliers	Yes	No	Don't know
Do you have alternative suppliers for critical equipment/ stores/ parts/ goods/ products etc?			
Do you have an arrangement with your critical suppliers where they will inform you if they cannot make a delivery?			
Do your suppliers have a business continuity plan?			
Do you have your suppliers correct contact details – both office hours and out of office hours?			
Do you have the correct contact details for all your main customers?			
Do you have any key customers who you will need to be in constant contact with during a crisis?			

Other	Yes	No	Don't know

What are the impacts on my business?

Consider how you would maintain business under circumstances such as:

- loss of premises or lack of access to premises
- loss of staff
- loss of key suppliers
- loss of, or interruption to, utility supplies
- loss of, or interruption to, IT and telecommunication systems
- loss of specialist equipment
- disruption to transport

What would the impact would be for:

- First 24 hours
- 24 – 48 hours
- Up to one week
- Up to two weeks
- Longer than a month

What are your critical activities?

- What services do you provide?
- What products does your business supply?
- Do you have any statutory responsibilities?
- Are there any financial/legal implications if your product/service is impacted?
- What are the priorities of these activies?

For each of your businesses critical activities;

- What is the priority?
- How long can you cope without that activity?
- What difficulties might you face?

Scenario: Loss of Accommodation

Things to consider:

- How would a total loss of your workplace, temporary loss of access affect your business?
- Are your evacuation plans understood and well rehearsed by all your employees?
- Are there any potential risks from surrounding premises which may affect your business?
- What are your critical activities that would be impacted by a loss of your workplace?

What are your next steps?

- How will you update your plan?
- Do you need to consider any actions i.e. staff awareness, evacuation procedures, etc.
- Do you need any external advice, e.g. Fire Safety Assessment.

Exercise: Loss of Accommodation

Under this type of scenario, the normal place of work is closed for normal business activities either short term or long term. Causes may include: power failure, road closure, fire, flood, bomb threat , water outage, gas leak, bomb alert, structural damage or area evacuation

Questions

1. What are the likely immediate effects of the incident scenario on your businesses ability to operate normally? What are the immediate actions required?
2. How will you minimise the impact on critical activities?
3. What are your responsibilities with regard to the welfare of your staff?
4. What are the workaround options in this scenario especially for the most essential services you provide?
5. How will you maintain continuing communications with your staff, customers, relatives or others. Where do you keep contact details?
6. What further contingency arrangements need to be considered?

Exercise: Loss of IT

Under this scenario supporting IT resources are affected including IT network outage loss of IT files technology connection outage, loss of data, system application outage, telecoms outage. These may be long term or short term disruptions.

Questions

1. What are the likely immediate effects of the incident scenario on your businesses ability to operate normally? What are the immediate actions required?
2. How will you minimise the impact on critical activities?
3. What activities rely on your IT?
4. What are the workaround options in this scenario especially for the most essential services you provide?
5. How will you maintain continuing communications with your staff, customers, relatives or others. Where do you keep contact details?
6. What further contingency arrangements need to be considered?

Scenario: Loss of IT

Things to consider:

- Do you have back ups of your systems?
- Are all your contacts/plans/critical data only stored digitally?
- What activities rely on having access to IT
- Remember IT can include your computers, internet access, telephone networks, etc.

What are your next steps?

- Ensure computers and memory devices are encrypted
- Ensure passwords are not shared
- Keep security software up-to-date
- Password protect confidential documents
- Keep confidential documents locked away
- Keep hardcopy back-up documents in a secure location
- Lock access to computers when not in use

Scenario: Loss of Staff

Things to consider:

- Who are your key members of staff?
- Can staff work from alternative locations?
- Do other staff members understand how to do key activities?
- How do you communicate with staff?
- Where are your staff based in relation to your workplace?

What are your next steps?

- Ensure all staff are trained in other key roles
- Re-task staff from non-essential roles
- Consider use of agency staff or contractors
- Postpone any non-essential activities
- Consider outsourcing activities where applicable
- Ensure all staff contact details are up-to-date

Exercise: Loss of Staff

Under this type of scenario, supporting staff resources are affected because of contagious illness, strike, transport outage, adverse weather, etc.

Questions

1. What are the likely immediate effects of the incident scenario on your businesses ability to operate normally? What are the immediate actions required?
2. How will you minimise the impact on critical activities?
3. What are your responsibilities with regard to the welfare of your staff?
4. What are the workaround options in this scenario especially for the most essential services you provide?
5. How will you maintain continuing communications with your staff, customers, relatives or others. Where do you keep contact details?
6. What further contingency arrangements need to be considered?

Case Study; Romsey Industrial Estate

In 2013/14 Hampshire experienced widespread flooding which impacted homes, businesses and highways.

Several businesses in Romsey were impacted by the flooding as they found themselves unable to take deliveries or ship items from their warehouses as the access routes where flooded, after the flood waters had receded in the surrounding area.

They had not considered that a flood event would impact their critical activities.

A number of businesses worked together to improve their business continuity by investing in temporary flood defence measures that would enable them to keep the road open following any future flooding.

Emergency Pack for your Business

If you had to evacuate the premise, having some key details at hand, or stored off site will make a significant difference in how quickly you can react

This could contain:

- ✓ Business continuity plan (BCP)
- ✓ Contact details for insurance, customers, suppliers, landlord etc to be contained in the BCP
- ✓ Spare copies of BCP appendices, log sheets, contact lists etc
- ✓ Building plans (if appropriate)
- ✓ Laminated action cards
- ✓ High visibility vests
- ✓ Salvage inventory
- ✓ Basic toolkit
- ✓ Phone chargers
- ✓ Pen and paper – to write down anything important

Resources available

- Local Resilience Forum – www.hantsprepared.co.uk www.iowprepared.co.uk
- Your local Council - https://www.hants.gov.uk/community/emergencyplanning/prepareyourbusiness https://www.iow.gov.uk/Council/OtherServices/Emergency-Management/Business-Continuity
- Community Risk Register
- Business Continuity Institute - www.thebci.org
- Government Toolkit - https://www.gov.uk/guidance/resilience-in-society-infrastructure-communities-and-businesses#business-continuity
- From your library;
  - Business continuity for Dummies (BCI and Cabinet Office)
  - Disaster Recovery Handbook (Wallace and Webber)

Want to get in touch?

Contact us:

E: HIOWLRF@hants.gov.uk

T: 01962 846846

Or write to us:

Emergency Planning and Resilience Team

EII Court South

Hampshire County Council

Winchester

SO23 8UJ

www.hantsprepared.co.uk
www.iowprepared.co.uk

Hampshire and the Isle of Wight
Local Resilience Forum