

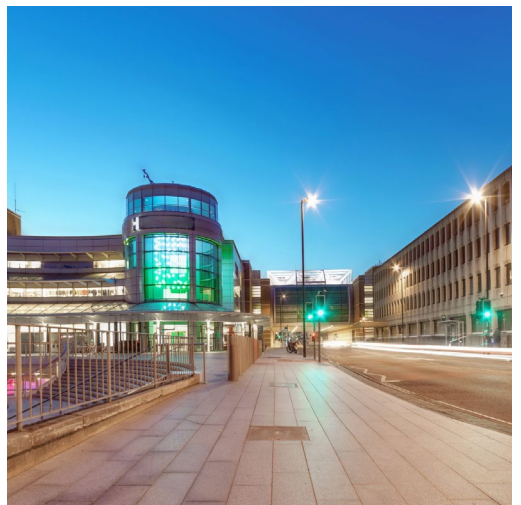


Business Continuity Handbook

PREPARE. RESPOND. RECOVER.

LRF

Local Resilience Forum
Hampshire & Isle of Wight



Introduction

What is Business Continuity?

Business continuity is all about preparing your organisation to handle disruptions smoothly and bounce back quickly. It can help build resilience, protect your reputation, and safeguard your organisation.

Business continuity means knowing your organisation and empowering your teams to respond confidently when challenges arise, whether it's a fire, flood, power outage, or loss of access to your premises.

This booklet is for small and medium organisations, including voluntary, community and faith groups, to start thinking about business continuity and start taking the first steps on being prepared.

For more information visit the Hampshire and Isle of Wight Local Resilience Forum (LRF) website: www.hiowprepared.org.uk 

Planning for the Unexpected

How well your organisation recovers from a challenge depends on how effectively you plan.

Have you thought through the key areas that keep your organisation running?

These are usually the main parts:



People

Are your staff safe, informed, and ready to act?



Communications

Can you easily talk to your staff, customers, suppliers? Do you know what to say?



Places

Where are all your organisation's locations? What if all or some weren't accessible?



Equipment & Stock

Where are these kept and what do you need?



IT & Data

Do you have back-ups; can you access the essentials if something happens?



Money

Are you insured, can you quickly buy essentials if there's a disruption?



Support & Advice

Who can you ask for help?

Why you need a Business Continuity Plan (BCP)

Once you've thought about the critical people, places, and finances that keep your organisation running. It is usually a good idea to write down it all down in a plan.

Your Business Continuity Plan (BCP) is your go-to guide when things go wrong. It brings together all the critical information you'll need to respond quickly, recover smoothly, and keep your business running.



Having a BCP in place means:

- ✓ You'll handle disruptions more effectively
- ✓ You're likely to save money by minimising downtime
- ✓ You'll protect, and even strengthen your reputation by supporting your customers when it matters most



How do we develop a BCP?

The best way to develop a BCP is to have a few people in your organisation read this booklet and then sit down together and think through these questions and steps.

Step 1

What does your organisation provide / deliver:

- ✓ What is the aim of your organisation?
- ✓ How do you go about achieving your aim? Think about what you do in your organisation (your activities) and prioritise these; what activities are the most critical (Critical Activities).
- ✓ What does your organisation do to deliver those critical activities? Think about people, buildings, communication systems, IT, suppliers, specific knowledge or training.



Develop your own BCP
with these 6 easy steps

Step 2

What are the risks?

- ✓ Which risks do you think could impact you? Common things would be weather, utilities outages, cyber impacts. For more information look at the National Risk Register, and the HIOW LRF website for local risks.
- ✓ There are other potential risks to organisations, such as reputational risks, operational risks, strategic risks and supply chain risks.
- ✓ List the risks you think could impact your organisation and decide if you need to plan for those risks happening, or if you are happy to accept the risk happening.
- ✓ Write down how each of these risks would impact your organisation's aim and activities (as in step 1).

Step 3

Agree the big picture

- ✓ Who has responsibility for dealing with these risks if they happen.
- ✓ How are they alerted if the risk happens? You might want to make sure people are available out of hours if you need to.
- ✓ What are the first actions people will take if a disruption happens, and who is responsible for those actions?
- ✓ Are there key people and places that need to be thought about first.
- ✓ Revisit your aim and activities, what will be the priority if something goes wrong.

Step 4

Write it all down

- ✓ Use the information you have gathered, and guidance available to write the plan. The next section suggests some topics to consider.
- ✓ Print a copy of your plan in case of IT / power failure and ensure staff know where it is kept.

Step 5

Don't leave it on a shelf

- ✓ Share and explain your plan to people in your organisation. This can be done through awareness sessions.
- ✓ Regularly test your plan through discussions, at people's desks or live exercises. There are scenarios that you can use at the end of this document.
- ✓ People should know what to do if something goes wrong, and the first actions to take. Knowing this will help them respond when incidents happen.

Step 6

Keep it up to date

- ✓ Once you've written it, you need to make sure it's stays up to date. Your organisation may start working in a new location, hire new staff or identify a new risk.
- ✓ Review your plan on a regular cycle, 6 months or a year.



Suggested sections of your Business Continuity Plan (BCP)

- ✓ Introduction
- ✓ Aims & objectives
- ✓ Core activities list, with their time frames. Include how long you could cope before getting this activity started again
- ✓ Prioritise activities considering what is critical, high, medium and low
- ✓ Known potential risks
- ✓ Plan triggers and activation (at what point does someone get a call and who do they call)
- ✓ Action cards for response (people might have specific jobs, or there might be specific things to do depending on the risk)
- ✓ Recovery process (how are you going to get back up and running)
- ✓ Key contacts, staff, customers, suppliers, other stakeholders



Suggested contents of an Emergency Pack?

If you had to evacuate the premise, having some key details at hand, or stored off site could make a difference.

It could contain

- ✓ Business continuity plan (BCP)
- ✓ Contact details for things such as insurance, staff, customers, suppliers, landlords, tenants
- ✓ Building plans
- ✓ High visibility vests / lanyards that identify people in the organisation and their roles
- ✓ Torches
- ✓ Bottled water / hand sanitizers / cleaning wipes
- ✓ Salvage inventory (you could consider videoing contents of your premises on a regular basis, so you know what's kept there)
- ✓ Phone chargers
- ✓ Pens and notebooks – to write down anything important

Loss of Staff

Loss of IT



Scenarios

Loss of Accommodation

Introduction

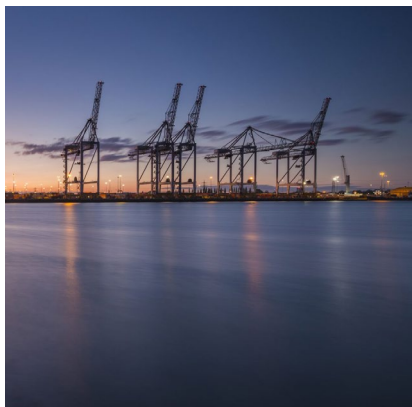
Once you've written a plan you can test it using these scenarios.

They are scenarios which could happen to your business.

Get people together to read through the scenarios and complete the exercises, using your Business Continuity Plan (BCP) to see how your organisation would cope.

Keep a list of things that went well or didn't go well during the test to change in the plan.

Test your plan with scenarios





Scenario

Loss of Accommodation

What would you do if you couldn't access your normal place of work?

Pick one of these scenarios:

Power outage - power goes off unexpectedly during the working day and is then off for 2 days.

Road closure - a main road near one of your critical sites has a significant accident, and traffic is at a standstill, you expect it to be closed for at least 8 hours, people travelling to and from that place are likely to be held up for hours.

Bomb threat - someone calls your reception and makes a bomb threat.

Flood - staff arrive in the morning to find a location completely flooded, with about 30cms of water (either weather flooding or burst pipe).

Gas leak - people in your building call the gas company because they smell gas, they are advised to evacuate immediately and once the gas company get there it's likely to be up to a week until they can re-enter.

Top tip!

Decide where you will meet or identify a backup location.

Questions

1. Using your Business Continuity Plan (BCP) or other procedures is it clear what the first actions would be in this scenario?
2. What do you think would happen to your organisation's aim and critical activities in this scenario? Is it clearly stated in your plan?
3. Do you have actions in your plan to minimise the impact on critical activities?
4. What are your responsibilities to the welfare of your staff?
5. How will you contact your staff, customers, and others key people. Are the contact details in the plan up to date?
6. If you need to evacuate in the scenario are there plans in place, and have they been tested recently?

When you have worked through this scenario, ensure everything is covered in the plan. If it's not, update the plan, run another scenario, and reach out for additional support.



Scenario

Loss of IT

What would you do if you experienced a loss of IT capability?

Pick one of these scenarios:

Ransomware via phishing email - someone in your organisation received a credible email, when IT helps them open the attachment it delivers malware into your systems, you get a ransomware request for a significant amount of money.

Data lost from your IT systems - critical files are being deleted from your IT system, it turns out a key employee was using the same password and email for their social media accounts, and they've been hacked.

Your website is redirecting people to malicious content - the vulnerability that allowed someone to do this was notified to you. To take down the links will require IT expertise.

Internet connections and telecoms aren't working - The first people to start work in the office can't access cloud based services, phones, Wi-Fi and payment machines are all dead.

Top tip!

Some of these scenarios are based on the **National Cyber Security Centre's resource** [🔗](#), Exercise in a Box.

Questions

1. Using your Business Continuity Plan (BCP) or other procedures, is it clear what the first actions would be in this scenario?
2. Do you know which people in your organisation have access to these systems? What would they do if this scenario happened?
3. How will you contact your staff, customers, and others. Are the contact details in the plan up to date?
4. What would you do if you couldn't access key information because of system outages or elements being compromised?
5. Do you have alternative options for your critical IT systems? Do you have paper systems, or other means of payment / ordering? Are these in your plan?
6. What training have you given your staff in IT security and restoration?

When you have worked through this scenario, ensure everything is covered in the plan. If it's not, update the plan, run another scenario, and reach out for additional support.



Scenario

Loss of Staff

What would you do if your staff couldn't get to work, come into work, or leave work?

Pick one of these scenarios:

Sickness - after a team night out a number of people have been afflicted with the same severe symptoms, with a couple being so seriously affected they are in hospital.

Strike action - members of your organisation are taking legal strike action; there is publicity and leafleting near your premises.

Snow - heavy snow has been falling and more is forecast over the next two days, some people are at work and worried about getting home, others don't think they'll be able to get in.

Fuel - there's been some issues heavily reported about filling stations not having fuel, your staff and your company vehicles are struggling to fuel and get to work and to other places.

Storms - extreme weather is forecast, with advice to only travel if necessary, many schools are going to be closed the next day because of the forecast.

Top tip!

Pick one of these scenarios, or think about how your organisation dealt with the Covid-19 pandemic.

Questions

1. What does your Business Continuity Plan (BCP) have in it that helps with this scenario?
2. Where do your critical activities take place? Can people work from other locations or from home?
3. What are your responsibilities with regard to the welfare of your staff? What about if they can't get in?
4. What are the alternative options in this scenario especially for the most essential services you provide?
5. How will you know what's happening, who is able to work or not, what teams can do their job and which ones can't?
6. What further contingency arrangements need to be considered?

When you have worked through this scenario, ensure everything is covered in the plan. If it's not, update the plan, run another scenario, and reach out for additional support.




Further resources available

Local Resilience Forum


www.hiowprepared.org.uk 

Your local Council

www.hants.gov.uk/community/emergencyplanning/prepareyourbusiness 

www.iow.gov.uk/keep-the-island-safe/emergency-management/business-continuity 


www.southampton.gov.uk/environment/emergencies-and-severe-weather/emergency-planning 

www.portsmouth.gov.uk/services/business/running-a-business/business-continuity-in-an-emergency 

Business Continuity Institute

www.thebci.org 

Government BCM Toolkit

https://assets.publishing.service.gov.uk/media/5a7b283de5274a34770e9d01/Business_Continuity_Management_Toolkit.pdf 

National Cyber security Centre advice and guidance

<https://www.ncsc.gov.uk/section/advice-guidance/small-medium-sized-organisations> 

Checklist exercise

Once you've worked through this booklet, you can run through the following checklists.

Checklists 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**, consider if these are relevant to your business, and if they are, find out more to include in your plan.



Work through the lists for yourself

General Considerations

Checklists of things to consider	Yes	No
Is Business Continuity management endorsed by the owners / partners / board?	<input type="checkbox"/>	<input type="checkbox"/>
Is there someone in your organisation who will have responsibility for leading on Business Continuity?	<input type="checkbox"/>	<input type="checkbox"/>
Do you know the critical activities your business delivers and what the impact would be if they were disrupted?	<input type="checkbox"/>	<input type="checkbox"/>
Do you have a Business Continuity Plan (BCP)?	<input type="checkbox"/>	<input type="checkbox"/>
Is the plan documented clearly and easily accessible, do staff know their role in it?	<input type="checkbox"/>	<input type="checkbox"/>
Have you exercised your plan within the last 12 months?	<input type="checkbox"/>	<input type="checkbox"/>
Do you regularly review and update your plan including learning from incidents?	<input type="checkbox"/>	<input type="checkbox"/>
Are your staff trained in activating and operating your plan?	<input type="checkbox"/>	<input type="checkbox"/>
Do you have a system or process in place to contact key individuals including staff, suppliers etc?	<input type="checkbox"/>	<input type="checkbox"/>
Have you prepared an emergency pack?	<input type="checkbox"/>	<input type="checkbox"/>



Equipment and documents

Checklists of things to consider	Yes	No
Have you identified your key equipment?	<input type="checkbox"/>	<input type="checkbox"/>
Do you have contingency plans in place to cater for the loss/ failure of key equipment?	<input type="checkbox"/>	<input type="checkbox"/>
Do you regularly update an inventory of your company equipment?	<input type="checkbox"/>	<input type="checkbox"/>
Do you have controls over the movements of your company equipment?	<input type="checkbox"/>	<input type="checkbox"/>
Do you regularly copy/backup your information?	<input type="checkbox"/>	<input type="checkbox"/>
Are your critical documents adequately protected?	<input type="checkbox"/>	<input type="checkbox"/>
Do you have copies of your critical records at a separate location?	<input type="checkbox"/>	<input type="checkbox"/>



Buildings and people

Checklists of things to consider	Yes	No
Do you have emergency evacuation procedures for your building(s)?	<input type="checkbox"/>	<input type="checkbox"/>
Do you have access to your building at all times?	<input type="checkbox"/>	<input type="checkbox"/>
Do you have fire safety procedures in place?	<input type="checkbox"/>	<input type="checkbox"/>
Do you have access to alternative workspace(s) to use in an emergency?	<input type="checkbox"/>	<input type="checkbox"/>
Have you got a list of all employee contact telephone numbers and home addresses? Ensure this is stored securely (GDPR).	<input type="checkbox"/>	<input type="checkbox"/>
Have your staff been given specific roles in the event of a crisis?	<input type="checkbox"/>	<input type="checkbox"/>
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?	<input type="checkbox"/>	<input type="checkbox"/>
Do you have members of staff with first aid or medical training?	<input type="checkbox"/>	<input type="checkbox"/>
Have you identified and considered the risks from your surrounding area and businesses? E.g. Flood risk.	<input type="checkbox"/>	<input type="checkbox"/>



Information Technology

Checklists of things to consider	Yes	No
Are your IT systems critical to the running of your business?	<input type="checkbox"/>	<input type="checkbox"/>
If your IT systems went down do you have manual processes that could maintain critical documentary/administrative functions?	<input type="checkbox"/>	<input type="checkbox"/>
Do you know how long it would take to recover IT functions if your system went down?	<input type="checkbox"/>	<input type="checkbox"/>
Who would restore your system if it went down and do you have their contact details?	<input type="checkbox"/>	<input type="checkbox"/>
Do you have a tested IT disaster recovery plan?	<input type="checkbox"/>	<input type="checkbox"/>
Is your computer anti-virus software up to date?	<input type="checkbox"/>	<input type="checkbox"/>
Are documented IT security policies and procedures in place?	<input type="checkbox"/>	<input type="checkbox"/>

Checklists of things to consider	Yes	No
Are all your computer users fully aware of email and internet usage policies?	<input type="checkbox"/>	<input type="checkbox"/>
Is your company system part of a larger network?	<input type="checkbox"/>	<input type="checkbox"/>
Do you know how many platforms / servers / applications or operating systems support critical business functions?	<input type="checkbox"/>	<input type="checkbox"/>
Does more than one person know how to use your IT system, including where critical documents are electronically stored etc?	<input type="checkbox"/>	<input type="checkbox"/>
Do you have vital computer information stored or backed up to the cloud or held off premises?	<input type="checkbox"/>	<input type="checkbox"/>



Customers and suppliers

Checklists of things to consider	Yes	No
Do you have alternative suppliers for critical equipment / stores / parts / goods / products etc?	<input type="checkbox"/>	<input type="checkbox"/>
Do you have an arrangement with your critical suppliers where they will inform you if they cannot make a delivery?	<input type="checkbox"/>	<input type="checkbox"/>
Do your suppliers have a business continuity plan?	<input type="checkbox"/>	<input type="checkbox"/>
Do you have your suppliers correct contact details – both office hours and out of office hours?	<input type="checkbox"/>	<input type="checkbox"/>
Do you have the correct contact details for all your main customers?	<input type="checkbox"/>	<input type="checkbox"/>
Do you have any key customers who you will need to be in constant contact with during a crisis?	<input type="checkbox"/>	<input type="checkbox"/>

Create your own checklist

Be specific to your business

Other	Yes	No
	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>

This document has been created by Hampshire and Isle of Wight Local Resilience Forum.

For more information on local risks, emergencies, and how to prepare.

Visit HIOWprepared.org.uk



Local Resilience Forum
Hampshire & Isle of Wight

Hampshire and Isle of Wight Local Resilience Forum

Fire and Police Strategic
Headquarters

Leigh Rd, Eastleigh SO50 9SJ