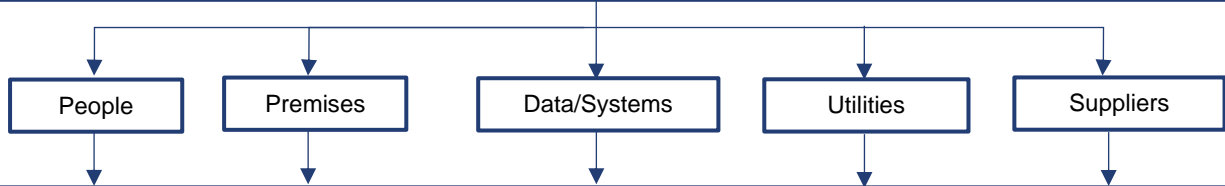


WOULD YOU BE READY?

Take 10 Minutes to develop an Emergency Plan

1. Understand your business critical functions and activities

List your business critical functions and activities ie without which your business will be unable to deliver products and/or services and could ultimately fail



2. Timeframes

What is the maximum period of time these critical functions and activities could be suspended without causing your business lasting damage? (e.g. 24 hours, 7 days, 14 days etc.)

3. Assess your risk

Consider what **impact** a disruptive event such as a cyber attack or a flood could have on these critical functions and activities and the **likelihood** of them occurring - categorise as **high, medium or low risk** to help prioritise action e.g.

- Key staff are unavailable
- Loss of customer data
- Unable to access IT systems
- Unable to access premises
- Major supplier goes out of business
- Telecommunications outage
- Loss of electricity, water or gas
- Transport networks are disrupted

4. Reduce your risk

What preventative measures can you put in place to help reduce the impact of a disruptive event in each of these areas?
You can use the checklist overleaf as a prompt

5. Develop an Emergency Plan

The plan should include a primary and deputy contact to implement the plan as well as triggers for when the plan should be invoked. The plan must be documented and reviewed regularly - at least every six months

6. Communicate and rehearse your Emergency Plan

Include the plan in staff induction and regular staff training. Regularly test and rehearse elements of the plan.
Consider sharing your resilience plan with your suppliers and local business network

7. Create an Emergency Communications Plan

This plan should include key contacts, a chain of command, and processes for tracking and communicating business and employee status. It should also be reviewed and updated regularly



10 Minute Emergency Plan – Checklist

Stay informed	check
Check your insurance and make sure you understand the terms and conditions and any exclusions	
Check live alerts – sign up for flood warnings and Cross Sector Safety and Security Communications	
Download the British Red Cross Emergency app	
Check your flood risk – coastal, river, rainfall/run-off	
People	check
Identify and document key procedures and details of staff with key skills and knowledge	
Consider contingency training for key roles/functions	
Consider Health & Safety staff training including First Aid	
Consider remote working policy	
Nominate a primary and deputy contact to implement your Emergency Plan	
Communicate your Emergency Plan to staff and rehearse	
Premises	check
Understand site evacuation routes and undertake weekly security checks – IT / Fire alarm / Security system	
Consider back up premises a) 3rd party provides recovery site/equipment b) reciprocal agreement with another organisation	
Consider flood and fire protection measures	
Create an emergency contacts list for tradespeople such as glaziers, carpenters and electricians	
Prepare a flood kit – supplies for <3 days and copies of key documents including your Emergency Plan and contact lists	
Develop a dynamic lockdown procedure	
Data	check
Use secure devices and software which are kept up to date	
Use passwords to protect your data	
Protect against viruses and malware	
Regularly provide cyber security training for your staff	
Regularly back-up digital data and keep a copy offsite and/or in the cloud	
Scan paper copies/key documents and store copies offsite	
Utilities	check
Consider back-up utilities; energy, water and telecommunications	
Consider portable generators - provided by a 3rd party	
Suppliers	check
Create a contact list of current and alternative suppliers and diversify suppliers where possible	
Include in tender process/contracts the need for a supplier to have their own emergency/business continuity plans in place	
Share your Emergency Plan with neighbouring businesses and identify ways to provide mutual support	
Communication	check
Create contact lists and cascade plan:	
<ul style="list-style-type: none"> All staff and their emergency contacts (ie next of kin) Key customers and suppliers Insurer – claims manager Bank – relationship manager Neighbouring businesses that could provide support/may need to be informed about the disruptive event IT and cyber security support Electricity, gas and water (24 hour emergency) 	
Be prepared to use social media to communicate with stakeholders about your business disruption	