Business Continuity Plan vs. Contingency Plans:
An Essential Guide for Organisations

There is a common misconception that the Business Continuity Plan and Contingency Plans are the same, but this is not the case, and although they are essential companions, it is good to understand the differences. This is a brief introduction to the variances and how the two work together:

Aspect	Continuity Plan	Contingency Plan
Definition	A proactive plan that outlines how to maintain or restore essential business functions during and after a disruption.	The process of handling the immediate response to a critical incident or emergency to protect people, assets, and reputation.
Focus	Ensuring continuity of operations and minimising downtime.	Managing the immediate response, communications, and decision making during a crisis.
Timeframe	Covers preparation, continuity during, and recovery after a disruption.	Focuses on the initial response phase of an incident or crisis.
Scope	Broad, includes IT recovery, operations, supply chain, facilities, and more.	Narrower, focuses on immediate safety, communication, and reputation protection.

How they work together:

- The Contingency Plan is the first line of response, containing and managing the immediate incident.
- The Business Continuity Plan is activated to maintain operations and guide recovery efforts.
- Both are part of an organisation's overall resilience strategy, but they serve distinct purposes and timeframes.

Think of Crisis Management as the emergency response team putting out the fire, while the BCP is the plan for keeping the business running and rebuilding afterward.

A Contingency Plan typically addresses incidents such as:

- Natural disasters (storms, floods, earthquakes)
- Equipment or technical failures (power outages, AV equipment malfunction)
- Health and Safety emergencies (medical incidents, fires, security breaches)
- Supplier / contractor failures or cancellations
- Travel disruptions affecting key personnel
- Cyberattacks or data breaches
- Accidents or epidemics impacting workforce availability
- Product defects impacting reputation or requiring recalls

These plans provide predefined responses to these specific incidents, focusing on immediate actions and alternatives to minimise disruption.

A Business Continuity Plan is activated when there are events causing significant disruptions to normal business operations, that require maintaining or quickly restoring essential functions. Common causes include:

- Natural disasters rendering facilities inaccessible
- Cybersecurity incidents impacting data or systems access
- Extended power outages or utility failures
- IT system or network outages impacting critical services
- Supply chain disruptions affecting production or delivery
- Situations impacting a large portion of the workforce (e.g., pandemics)
- Any event that threatens ongoing service delivery or operational stability

The continuity plan aims to keep the business operational during these disruptions, minimizing downtime, financial losses, and protecting customer trust.

Failing to plan is planning to fail, know your plans and how they work together

Business Continuity Assure
www.bcassure.co.uk
contact@bcassure.co.uk