HORIZONSCAN

RISK - RESILIENCE - READINESS

# Good Practice Guide 1 : Resilience through Business Continuity Planning

## Does the organization have a Business Continuity Plan in place?

**Business continuity planning** is the process of creating systems of prevention, response and recovery to deal with potential threats to a company. In addition to prevention, the goal is to enable ongoing operations before and during execution of any recovery.

A **Business Continuity Plan (BCP)** is a guidance document that supports the maintenance of the business during a crisis event and throughout the recovery phase . A **validated** (through testing) Business Continuity Plan should be embedded within the organization and has ownership.

The BCP should be developed by a group representing the key functions of business and include ongoing peer/managerial review. They should identify potential **risk** that may cause business interruption. From these risks they should then viewed as potential 'impacts' to the site. This is called a **Business Impact Analysis (BIA)**.

The BCP will outline strategies and tactics that will support the business during the initial phases of a crisis event. It will define response, with roles and responsibilities.

It will guide the business into crisis stabilisation and define priorities and detail information to recover the business.

Once the BCP is developed. It needs to be validated and then embedded into workings of the business, and the appropriate stakeholders.

Validation is usually carried out through a range of processes including tabletop exercising and crisis simulation exercises. This should reassure the organisation that the plan is fit for purpose and staff are competent in its enactment.

## The Business Continuity Plan contains a list of people with defined roles and responsibilities?

Defining roles and responsibilities in a Business Continuity Plan will enable quick activation, engagement and focus on key tasks the Crisis Command Team must fulfil. This should be pre-agreed, and the roles and responsibilities reflect the key functions of the business.

Any staff member who is identified as having a pre-agreed role will require training to ensure they maintain competence.

There are potentially two groups of responders to most Crisis events. They are the Crisis Command Team (CCT) and the Emergency Response team (ERT). If you are identified as a member of either of these, you should ensure you engage in the appropriate training to ensure and maintain competency.

It is important to acknowledge that at the earliest stages of a crisis the correctly trained person may not yet be available. In this circumstance staff may be expected to work in areas that may be unfamiliar to them, until such times as a more suitably trained person is available.

Specific responsibilities should be detailed and allocated in the BCP. These may be functional (i.e. Safety, finance, IT) or a part of strategic or tactical response structure.

It may be appropriate to include how to contact any staff member who has a pre-agreed role. But be aware of any personal/data compliance issues with including names and home addresses.

## Does the Business Continuity Plan identify the internal and external risks relevant to the organization?

Risk can include a wide variety of impactful events. These can be caused by internal or external factors.

Internal risks are usually events isolated to the site. This could include fire, flood, accident/injury, weather event.

External risks may include trade embargoes, currency fluctuation, political unrest.

Often internal and external risks can occur simultaneously to create a range of Business Impacts. It is appropriate to understand these impacts and not just the risks.

## Does the organization have an offsite location for the Crisis Response Team to use, that are identified in the Business Continuity Plan?

Many Crisis events will create a physical impact to the Site. This may render the onsite location (or access to it) unavailable. Alternative arrangements should therefore be in place.

An off-site location is a pre-agreed alternative location that can be used to set up a response room if the facilities on site are not able to be used. Denial of access to site is a common cause of Business Interruption. It is important that the Crisis team have a safe location to respond to any business interruption events. Consideration to the location of the off-site resource should be given; If it is too close it may be impacted by the same event impacting your site. If it is too far away it may cause unnecessary

delays in setting up the resource and maintaining staffing. If it is too close it may be impacted by the same event causing your site interruption.

The offsite location should be tested to ensure it has the correct facilities for communications, information gathering and recording. It must have guaranteed availability 24 hours a day/ 365 days a year. This location should be used for an annual exercise to ensure all systems work as required and staff are suitably trained in using the off-site location.

A Service Level Agreement should exist with the owners of the offsite location.

## Does the site/organization have defined Recovery Time Objectives (RTO's)?

Businesses need to understand that Crisis, business interruption events and recovery are built around agreed timeframes. RTO is a measurement of your tolerance for non-production/downtime.

RTO should be informed by Business Impact Analysis. Business impact analysis is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident, emergency or other unplanned events.

RTO's must be included in the Business Continuity Plan and will state the time frames that are expected to recover areas of the business. They must be reviewed annually and should be owned and supported by Senior leadership.

The RTO, along with a business impact analysis, provides the basis for identifying and analysing viable strategies for inclusion in the Business Continuity Plan. Viable strategy options include any which would enable resumption of a business process in a time frame at or near the RTO.

## The Business Continuity Lead is competent and confident in the role?

The role of Business Continuity Lead is critical to protecting and mitigating the harm from business interruption events. As such it is critical that this person is competent in this role.

Each site will require a functional leader for Business Continuity. This person carries out the day-to-day Business continuity management and administration. They report to senior leadership.

It is acceptable that Business Continuity Lead may also carry out other roles and functions in the business. They are recognised within the business as responsible for Business Continuity and there is ownership. To be competent they must be suitably trained in this role.

Competence and understanding of Business Continuity should be regularly demonstrated and updated. Appropriate records of this competency should be maintained.

## GLOSSARY

**Resilience**

Business resilience is the ability an organization has to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets and overall brand equity.

**Emergency Management:**

Emergency management is the organization and management of the resources and responsibilities for dealing with all human aspects of emergencies (preparedness, response, safety, mitigation, and recovery). The aim is to reduce the harmful effects of all hazards, including disasters.

**Crisis**

Inherently abnormal, unstable and complex situation that represents a threat to the strategic objectives, reputation or existence of an organization

**Crisis Management**

Crisis Management is the process by which a business or other organization deals with a sudden emergency situation.

**Crisis Response Team**

A team of people (usually local managers) who are able to come together quickly and enact the initial response plans for a crisis event

**Invoking**

The formal declaration of starting of a process of planned response(s) to an emergency or crisis event.

**Emergency Action Plan (EAP**)

An agreed, rehearsed set of responses for all managers, responders, staff and visitors to be enacted should a specific emergency event take place (i.e. Fire, Hurricane warning)

**Business Continuity Planning (BCP)**

Business continuity planning (BCP) is the process involved in creating a system of prevention and recovery from potential threats to a company. The plan ensures that personnel and assets are protected and are able to function quickly in the event of a Crisis

**Business Impact Analysis (BIA)**

A Business Impact Analysis is a process that identifies and evaluates the potential risks & impacts of natural and man made events on business operations. The Business Impact Analysis will identify those risks and help define response.

**Resilience Exercise**

An exercise or simulation that tests the efficacy and ability of the organization to respond to an unplanned business interruption/crisis/emergency using existing resilience plans (EAP/BCP's)

**Emergency Responders / Teams (ERT)**

Trained individuals or team members who have specific duties during an emergency response to keep the site, equipment, stock or others safe.

**Business Continuity Lead**

A Leader (or manager) who has a responsibility to the site / organization to ensure business continuity practices and processes are developed, administered, tested and reviewed.

**Enterprise Risk Management (ERM)**

A function within the organization that assesses and reviews strategic (and macro) risks to the business. ERM do not usually address operational risk.

**Recovery Time Objective (RTO)**

The Recovery Time Objective (RTO) is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

**Data Risk Exposure (Cyber)**

Data risk is the exposure to loss of value or reputation caused by issues or limitations to an organization's ability to acquire, store, transform, move, and use its data assets. This may also include protection of customers data.