Good Practice Guide 2 : Resilience through Response

The site has conducted an internal resilience exercise in the last 12 months?

The planning process should be validated through a series of **practical exercises**. This will ensure that the plans content is appropriate and can be practically enacted.

Exercising can be carried out in a variety of methods, including full scale simulations, focused exercises, tabletop events and facilitated discussions.

These events should be carried out **regularly** and as a minimum **annually**. They should involve all **relevant managers and key stakeholders**.

These events should be logged and recorded, together with any appropriate action or improvement points. This process requires defined ownership at the appropriate level.

Capturing learning from exercises (and real world events) is a valuable part of improving organisational response capability.

Does the site have a formal process to activate the Crisis Response Team and /or Emergency Response Team?

It is essential that businesses have formal policy around how to respond to an emergency or Crisis event.

The formal process used to activate emergency or crisis response teams is called the **'invoking process'** This will identify the various stages of escalation and de-escalation. It will also include the specific responsibilities and the roles to be carried out by responders.

Policy will detail the invoking process, this will outline the required responders, actions and timeframes.

A pre-agreed and regularly tested invoking process will produce a faster, more cohesive response.

Does the site provide 24/7 response to a crisis?

Emergency and/or Crisis events can impact the business any time, day or night. It is therefor essential that the provision of an appropriate response should also be available during these times. This is not just the activation of emergency or crisis response teams but the availability of senior managers and other appropriate stakeholders.

There should be a reliable and pre-agreed process to ensure appropriate response at the required levels. This is usually achieved using on-call rota's or rosters.

This response should be tested, at least, annually and reviewed as part of continuous improvement.

A Crisis Response (Incident) Room is available?

Crisis response is best managed in a pre agreed location. For the Crisis Response Team to work effectively they should be in an environment where they are not disturbed by others.

This location should not have been directly impacted by the crisis event and is safe to use.

As part of pre-agreeing a location, an assessment should be undertaken that considers suitability to perform this function.

The location of the Crisis Response Room should be know to all crisis responders.

Does the organization have pre-prepared crisis response resources ready and available?

The Crisis Response Room must be suitably resourced to enable a quick and effective response.

It is critical that research and assessment is undertaken that identifies the appropriate resources that may be required to effectively manage a crisis event.

A suitable inventory of the required resources needed in the Crisis Response room is maintained and equipment tested regularly.

All potential crisis responders should be aware of the resources available and are trained annually in their use.

All resources should be regularly checked and 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.