HORIZONSCAN

RISK - RESILIENCE - READINESS

Good Practice Guide 3 : Crisis Communications

How are risks understood and communicated across the organization?

It is appropriate that all organizations understand the risks and potential impacts that they may be exposed to. These are usually identified and recorded in a **Risk Register**, which is regularly reviewed.
At a organizational level there should be a Crisis Communications Policy to dictate and control how communications are managed. Staff who supervise crisis communications should receive appropriate and ongoing training.
At a site level there should be designated and pre defined communication pathways to exchange and share information.
Known risks and their impacts should be well understood and communications strategies built around them.

Is there a process/mechanism in place for employees to report risks and concerns?

At site level there should be a formal process to allow risks and concerns to be reported. These should be reviewed and appropriate measure put in place to mitigate potential harm and impact.
This process should be appropriately documented and supported by policy/guidance.

The site has a process for receiving, documenting and responding to any national or regional risk advisory system (such as National Severe Weather Warnings, hurricanes, tsunami, wild fires) or equivalent?

To identify potential external impacts as soon as possible, information and alerts can be provided by local or national agencies to allow the organization/site to make early preparations which may prevent harm and mitigate impacts.
Monitoring and responding to information and alerts should be a formal process that is detailed in policy/guidance. There should be a process for senior management to discuss risk information received.

Does the organization/site have an external Crisis Communication Plan?

Communications to media, suppliers, customers etc during a crisis/emergency event are often very different from normal day to day communication.
Crisis communications can be complex and are needed at the earliest stage of a impactful event. Planning and pre-agreed media statements (in template form) will enable a quicker and more effective communications response. This will help mitigate and improve recovery times.
To ensure it is flexible and resilient, Communications Plans should have clearly identified 'alternative' communication methods and pathways.
These plans should be detailed in policy/guidance documents and should be tested and reviewed regularly.

Have key staff received practical training in internal and external crisis communications?

Key site staff who may have to undertake crisis communications should be pre agreed and identified as part of business continuity and crisis response planning.
They should receive appropriate and ongoing training.
They should rehearse the use of the required skills in simulations and exercises.
Those carrying out this role need a detailed understanding of all appropriate policy and guidance, as well as the local media profile.
Crisis communications will require interaction with all levels of the organisation as well as media outlets, suppliers, customers etc.

Does the organization/site have plans in place for internal crisis communications?

The site should have pre-agreed plans regarding internal communications to ensure staff are informed and can respond effectively and appropriately.
An internal communications plan should be detailed in local policy/guidance.

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.

Risk Register

A risk register is a document used as a risk management tool and to fulfil regulatory compliance acting as a repository for all risks identified and includes additional information about each risk, e.g. nature of the risk, reference and owner, mitigation measures. It plots the impact of a given event over of its probability.