HORIZONSCAN

RISK - RESILIENCE - READINESS

Good Practice Guide 7: Leadership Resources

Does the site have an identified senior leader (or similar) in place who is ready and able to direct a crisis event?

At an individual site level there should be an identified senior member of staff who is able and capable of leading the response to an emergency/crisis event. Ideally there should be more than one person and deputies should also be available. This role should be pre-agreed and clearly identified. The site should always have the ability to enact this role immediately. The person(s) identified to take this role should be trained and they should undertake regular testing. Best practice would demonstrate site crisis response leaders have received training and have been tested. This will be documented and recorded.

Have Crisis Response Team (CRT) members been trained, exercised, or tested (either training exercises or real disruptive events) within the last 12 months?

Crisis events will require a team to coordinate and command the site level response. They make up the CRT. These team members should be competent in responding appropriately to crisis events at site level. This can be achieved by ongoing training and development. Emergency leaders should have received training (or been exposed to a real emergency event) in the last 12 months. Best practice would demonstrate that there is a formal, structured and nominated crisis team training program in place and that cover is formally rostered to always ensure availability.

The leadership are fully aware of the risks/hazards to the organization/site?

At site level there should be a formal risk register that identifies risks and hazards locally. This should be maintained and owned by site leadership. All leaders at site should maintain an awareness and understanding of the risks. Best practice would demonstrate the risk register risk is maintained with leadership involvement and that priorities are documented.

What is the organization/site's current capability to anticipate, detect, respond, and recover from disruption?

The organization/site should be able to detect, respond and recover from any disruption and have adequate resources to do so. There should be systems, processes, and tools in place to detect and respond to disruptive events at all times when the premises are occupied or in use. There should be a pre-agreed written response and recovery plan to address certain higher risk events when detected. Best practice would demonstrate that detection and response systems are always in place, with a written recovery plan to address prioritised events. Staff are aware of what they need to do. Recovery plans are embedded into, or referenced by, the Business Continuity Plan

The organization/site's aims, and objectives are clearly defined and understood by employees?

Staff should all be aware of and understand the primary aims and objectives of the organization. These aims and objectives are clearly outlined in documentation and are widely communicated. Best practice would demonstrate that the aims and objectives are clearly defined and formally communicated to key staff on a regular basis.

Is sufficient support and resources assigned to emergency actions, business continuity and crisis management? (budgets, headcount etc)

There should be policies and processes detailing how emergency actions, business continuity and crisis management are supported and funded. Such should be supported by senior leadership with reviews and updates undertaken. Best practice would demonstrate Business Resilience as a functional area of the organization/site with budget available to drive improvements in these areas. Processes will require regular reviews and have defined ownership.

Evidence of continual improvement following a test or real crisis being incorporated into emergency action plans and business continuity plan updates?

Following any simulation exercise or real crisis event, there should be an 'after actions review' (AAR) process which can identify improvement areas that need addressing. Improvements made should be reflected in appropriate planning documents. Best practice would demonstrate that any learning outcomes from AAR are prioritized and implemented to seek improvements in performance.

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.