HORIZONSCAN

RISK - RESILIENCE - READINESS

Good Practice Guide 4: Risk

Has the site identified the key operational risks that may cause business interruption or require crisis response?

It is appropriate that organizations identify the key operational risks that have the potential to cause business disruption. Once identified a risk register should be compiled and regularly reviewed. Business continuity plans should reflect and outline these risks and detail mitigation strategies. These identified risks should also have documented emergency action plans, crisis response plans and recovery strategies. It is best practice to train against, and test these plans regularly.

Is life safety the number one priority of the organization/site and is this part of the organizations culture?

The safety of staff, visitors and others is recognized and acknowledged to be the priority during any emergency event. All staff are aware of their roles and responsibilities during emergency events. Emergency responders are trained to consider life safety as their primary objective before undertaking other tasks. It is considered best practice to reinforce this accordingly in all Emergency Action Plans and Business Continuity Plans.

Has the site undertaken a Business Impact Analysis (BIA) in last 12 months?

A business impact analysis identifies and evaluates the potential risks and impacts of both natural and man-made events on business operations. Identifying these risks will help to define responses.

A BIA has been completed, and a review undertaken in the past 12 months. It is considered best practice for there to be defined ownership of this process at site level.

Does the organization/site have an Enterprise Risk Management (ERM) function?

An Enterprise Risk Management function looks at all risk types but usually focusses on high level strategic and financial threats. It identifies, assesses, and provides appropriate response strategies and ongoing monitoring processes. The site management should be aware and facilitate basic response plans. It is considered best practice to have a policy to support this, with training for key staff to review existing risk and identify emerging risks.

Is your site in a known (or has experienced) a Nat-Cat event and/or likely to be impacted by natural disasters? (i.e. Wildfire, flood , earthquake or tornado)

In some geographical areas there may be an increased risk from these Natural Catastrophic events. Regional and State emergency and evacuation plans may be in place to deal with such events. Planning to deal with this type of event is essential. There should be established plans for all such identified risks. These should be regularly reviewed, updated and suitable training regularly undertaken. Best practice would demonstrate defined ownership and local plans which are structured around National, Regional or State guidance.

Does the organization/site consider regulatory compliance risks?

Regulatory compliance will ensure the site is not exposed to legal or contractual issues which could adversely affect production or its finances. Compliance should be driven by policy with requires regular reviews and updates. Best practice would demonstrate that the site leader has ownership and any required compliance issues are addressed and embedded in planning documents. Plans are structured around the National, Regional or State legislation or guidance.

Are quality control issues part of the organization/sites resilience planning?

Quality issues are known to cause supply chain interruptions. Having knowledge of suppliers, with guarantees of restoring supply chains with correct quality products with an agreed time frame will support resilience planning. Critical suppliers have provided documented anticipated re-supply times. Quality control is considered an aspect of Resilience planning. Best practice would demonstrate supplier’s recovery time objectives that are documented and annually reviewed, this is supported by Policy.

Are the geolocational risks considered as part of logistics and distribution?

Does the organization/site have goods and raw materials that need to be transported through areas that may pose specific threats? (i.e flood risk, earthquake zone, political). To overcome this, a diversified supplier approach could be considered. Best practice would demonstrate this is actively considered and annual reviews are completed. There are documented mitigation plans against identified threats.

Are macro risks considered?

Macro risk are usually outside an organization/site's control, examples may include credit, currency risks, terrorism, or political unrest. Senior managers should consider macro risks and have in place a documented risk process. Best practice would demonstrate a formal process to consider and analyse both current and emerging macro risks that are supported by a suitable Policy. The organization/site has an Enterprise Risk Management (ERM) Function.

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.