Cummins

HORIZONSCAN

RISK - RESILIENCE - READINESS

Good Practice Guide 5: Back Up and Contingency

Does the organization/site include transportation and logistics partners in their business continuity planning?

Business interruptions can occur within the transport and logistics chain, it is therefore appropriate that the resilience of any supply chain includes the movement of stock, products, and materials. The site should have preferred suppliers and contractual agreements with them. Theses should be reference within the business continuity plan. Best practice would demonstrate service level agreements are in place that are regularly reviewed, with the site leadership demonstrating ownership. These agreements would be detailed within the business continuity plan.

Does the organization/site assess risks in its logistics/ warehousing function?

There can be significant risks to goods when they are outside of the direct control of the organization. Logistic, warehousing and transportation risks can lead to interruptions in supplying customers. There should be a risk document maintained for these functions. Best practice would also outline mitigation plans with annual reviews taking place.

Does the Site have security function and security policies?

Site security will control access and egress to a site, as such these control measures will ensure minimum disruptions. A site security policy will define specific roles and responsibilities. There should always be a physical security presence when a site is occupied. Security should always work in accordance with the local security policy. Best practice would provide a 24-hour security presence by Security staff or a security company. There will be specific security performance standards, with security teams receiving training at least annually.

Does the site have alternative/multiple suppliers of goods/ raw materials?

Single source suppliers must be clearly identified. If a single source supplier suffered disruption or delay, this could impact the business or site. Having alternative suppliers may help prevent delays in production. Maintaining higher stock levels of raw materials and components could help mitigate supply chain interruption. If utilising single source suppliers, regular reviews should take place. There should be contingency plans to source from alternative/ back up suppliers. Contractual standards should exist with suppliers. Best practice would demonstrate there are contractual standards in place for all suppliers and that supplier performance standards are reviewed regularly. Increased stock levels are considered for key components.

Are your single source suppliers resilient?

Ensuring your suppliers have basic resilience will help ensure your own business resilience. Critical suppliers should always ensure that goods and service needs are punctually met. Resilience of key suppliers should be checked to ensure they have their own emergency plans and business continuity plans. Best practice would see an annual audit and validation program and that this should be documented. The outcomes of the audit and validation should be assessed, and appropriate actions taken.

Does your site have an alternative site they could relocate operations to if your current location cannot be used?

Having an alternative location that is readily available may allow the site to meet its contractual demands and obligations. An alternative site location should be available to support the basic business functions. Best practice would demonstrate availability with a formal arrangement in place for its use. The relocation process is documented, practiced, and rehearsed to improve business resilience.

Does the organization/site assess its data exposure risk? (Cyber risk)

Organization/site data is key to ongoing and stable performance. Loss, corruption, or theft of data will have serious consequences to a businesses ability to function normally and to maintain its reputation. This should be covered in a policy with documented assessments and that appropriate protection measures are active. Best practice would demonstrate defined ownership and control. New technology would be embraced, and data risk exposure is well understood and regularly audited.

Does the organization/ site have guaranteed repair times for its infrastructure? (i.e., Facilities, communications, utilities, plant and machinery)

Guaranteed response and repair times for infrastructure will be advantageous and reduce supply chain interruptions, it will inform potential downtime should a failure occur. Key infrastructure should be identified and documented with appropriate repair and maintenance programs in place. Best practice would demonstrate wide ranging repair and maintenance programs with pre-emptive renewal processes in place. There should be technical expertise on site. SLA exist for 3rd party landlord agreements.

Does the site/organization have contingency plans if significant numbers of staff are unable to work as normal?

Contingency plans exist to maintain production if existing staff levels are unexpectedly reduced for any reason (illness, industrial action, denial of access etc). Contingency pre-planning can ensure continued production and that movement of finished goods can be maintained at suitable levels. Best practice will demonstrate there are pro-active measures in place to prevent/mitigate this situation with plans annually reviewed.

Does your organization/site have fire safety and protection measures covering facilities, staff, stock and finished goods?

Protection from fire may include fire warning, detection, and protection measures such as fire suppression and sprinkler systems. There may be onsite fire wardens and fire response teams with an appropriate management and supervision system. Fire Risk Assessments are carried out, insurers advice is considered and reviewed. There is defined ownership with a management system. There is fire detection in place with risks covered with automatic detection and suppression systems. Regular staff training takes place. Best practice would demonstrate interaction with insurers and assessors and that existing fire safety standards exceed basic legal requirements. Staff response roles are clearly identified, and training undertaken.

Does your site/organization have general physical asset protection measures for the safety of staff, stock, and finished goods?

Asset protection measures may include flood protection, early warning systems, CCTV, and additional security measures. Insurer's advice is considered and reviewed. Asset protection has defined ownership. Asset protection is usually reactionary. Best practice would demonstrate asset protection being undertaken at all times, with defined ownership underpinned by policy. Regular information exchanges take place with the insurers.

Does the organization/site collaborate with its business partners to promote business resilience to ensure mutual prosperity?

Collaboration with suppliers will provide a better understanding of their business and will improve supply chain resilience. Discussions take place with all key suppliers to ensure their business resilience. Collaboration is encouraged. Best practice would demonstrate a regular review of all suppliers and formal meetings taking place with them. Resilience is mutually supported by all parties.

Does the organization/site have plans for the loss of key staff/talent?

Losing key staff and talent who take knowledge with them can impact a business. Such circumstances should be planned for to minimise interruptions. A plan should exist that demonstrates evidence of succession planning. Best practice would demonstrate a formal training program supported by policy with regular reviews. There are minimal points of failure identified with regard to the loss of staff.

What is the sites existing production capacity in relation to Cummins Parts and Products?

Having a diverse customer base will increase the site’s resilience, with failure of one customer having a smaller impact. 50% production for Cummins with remaining 50% made up of other customers. Reduction in this initial percentage to 30% will greatly increase site resilience.

Does the organization/site have key insurance programs?

Key insurance will include property and business interruption, environmental liability, and product liability insurance. Basic key insurance should be in place, with insurance assessment reports undertaken. Best practice would demonstrate defined site ownership responsible for maintaining and reviewing the key insurance program. Annual loss insurance reports are undertaken, and reports inform an improvement program.

Are potential bottlenecks identified and mitigated?

Bottlenecks can be identified in systems, processes and equipment. Infrastructure that may be unique, hard to replicate or highly specialised that becomes unavailable would seriously impact the function of the site. Critical bottlenecks should be identified using a formal process. Potential mitigations are assessed and when appropriate put in place. Best practice would demonstrate assessment as an ongoing formal process. There is a policy in place and senior management understand and mitigate potential bottlenecks.

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.