Making sense of risk
Disaster preparedness
Asia Pacific

Disaster recovery and business continuity plan

Liberty
Specialty Markets

Disaster recovery and business continuity plan

Disasters happen every day and affect businesses large and small; however, many businesses are under-prepared for a crisis.

Although disasters may be dramatic, newsworthy events, minor incidents happen more often and can still threaten the lives of employees and customers, your property, business operations and the environment. It is therefore crucial to plan well in advance of emergencies, in order to protect yourself, your employees and your customers from personal injury, your business from damage and protracted downtime, and the environment from unnecessary impact.

A well thought-out and documented Disaster recovery and business continuity plan can be the difference between a temporary business interruption and the complete and permanent disruption of operations. When disaster strikes, there is little time to react and even less time to develop and evaluate plans, teams and procedures for communicating key logistical information.

Having a carefully considered and well-rehearsed Disaster recovery and business continuity plan not only improves your company's chances of surviving a disaster, but also increases the confidence of your customers in your ability to continue providing the goods and services they rely on.

An organisation's disaster preparedness is also of interest to their insurance company, who may consider it as part of their risk assessment.

This guide is intended to help business owners and managers prepare in advance their business, premises and employees for a disaster in order to reduce business disruption or interruption.

Only you can develop an effective Disaster recovery and business continuity plan relevant to your business: your operations, hazards, and capabilities are unique, and your plan must be tailored to your own circumstances. No 'one-size-fits-all' plan will fit your needs perfectly; however, this guide describes a framework on which you can begin to build your plan.

Developing an effective Disaster recovery and business continuity plan involves the following steps:

- Establish a Planning Team
- Analyse risks and capabilities
- Develop a draft plan
- Test and implement the plan
- Update the plan

Establish a planning team

The success of a company's Disaster recovery and business continuity plan relies on implementation from the top down, which results in greater attention to risk at every level. All departments and levels should be represented on the Planning Team, with no individual acting in isolation. For full effectiveness, the Planning Team should be led by a Project Manager who has ultimate responsibility for writing and updating the plan.

Analyse risks and capabilities

After establishing a Planning Team, the next step is to *identify disruption-related risks*, the *likelihood* and *consequences* of their occurrence, and the *threats* they pose to your employees, property, environment, and business operations. Also consider risks that may affect your critical suppliers and customers. (A critical supplier is one that, if lost, would severely impact your business.)

Plan for impacts

Develop your plan for the impacts of selected risks, rather than for all potential risks, since the number of risks identified during your analysis may be vast. Attempting to develop a plan to address all possible disasters could be all-consuming and yet incomplete.

Complete a vulnerability analysis

Completing a vulnerability analysis with probability charting can help identify common impacts and critical business operations. There may be some elements of your business that are important, but not critical to meeting the company's basic goals of continuity of operations. For example, marketing, research and development and product testing can often be suspended for short periods of time without permanent consequences, allowing some resources to be redirected to other, more critical operations. As a priority, identify regulatory requirements for safety and disaster preparedness, and identify any available public sector resources.

Develop a draft plan

Each identified impact should have the following corresponding plans:

Strategic plan

A guide to activating recovery procedures

Emergency response plan

A guide to responding to the various impacts

Mitigation plan

Aguide to minimising or eliminating risks

Recovery plan

Aguide to focusing on priorities, vital resources and restoration

Strategic plan

The Strategic plan is a guide to activating recovery procedures and includes the plan's objectives, scope and structure, as well as the responsibilities of key personnel.

The following elements should be considered as part of the Strategic plan:

- Direction and control: the defined lines of responsibility and authority
- Communications: the way you will communicate with employees, the public, customers, suppliers and authorities
- Property protection: onsite security; security of information
- Community outreach: the capabilities of the organisation to help in a community-wide event
- Administration and logistics: the offsite command centre; relocation of operations and employees
- Financial requirements: the funding of each phase of the plan; maintenance of revenue streams
- Who is responsible for the budget?
- Who oversees the business recovery effort?

Consider these aspects as you develop your plan:

- What is the plan designed to achieve? (reduce business interruption; continue operations at alternate site)
- What is the scope of the plan? (one or multiple business units; local or widespread event)
- What is taken for granted in the plan? What is the confidence level? (outside response; use of infrastructure; in-house capability)
- What is the plan structure? How will it be accessed and used? (posted on web; paper documents available in kit; stored on USB drive)

Emergency response plan

The Emergency response plan is a guide to responding to the various impacts identified in the development phase. It clarifies what constitutes an emergency, how to report and respond to an emergency, the establishment of a command structure, and also provides safety program information.

The following elements should be considered as part of the Emergency response plan:

- Method to define levels of emergencies: coded signal; numerical; threat level
- Method to report emergencies: fire alarms; other alarms; PA system
- Evacuation: procedures and routes; evacuation rehearsals
- Procedure for the care of disabled personnel: identify personnel; plan for their safety
- Procedure for employees with a role in the plan: shut down; critical services
- Response team contact procedures: use of calling trees; social media
- Security procedures: identify authorised personnel; site security; manage funds
- Rescue duties: training; equipment
- Shelter-in-place procedures: identify hazards; manage shelter; shut down
- Media relations guidelines
- Medical alert procedures
  - onsite staff and training
  - notification procedures
  - list of potential medical impacts
  - access to medical services
  - availability of first aid and personal protective equipment

Mitigation plan

The Mitigation plan aims to: reduce or eliminate hazards that expose your company to danger; guarantee the response of critical suppliers (identified in the Strategic plan); ensure the safety of personnel; and provide guidance on site security and business resumption, including communication with customers.

The following elements should be considered as part of the Mitigation plan:

Pre-event

Measures designed to prevent or reduce the impacts:

- Consider agreements with key vendors
- Evaluate use of alternative sites and mutual aid agreements (with competitor)
- Review insurance requirements
- Prepare crisis kits
- Evaluate repair/replacement availability of critical production equipment and systems
- Evaluate critical raw materials and packaging replacement availability
- Evaluate ability to restore critical production utilities such as electrical power, steam, compressed air, cooling water
- Evaluate ability to restore critical computer and communications equipment and systems
- Identify facility access

During an event

Procedures to help manage the event:

- Consider safety
- Document events

Post-event

Measures designed to reduce operational downtime:

- Secure the site to prevent further damage
- Initiate agreements with suppliers and consider mutual aid
- Photograph the damage
- Keep track of expenses

Recovery plan

The Recovery plan should focus on short- and long-term priorities, access to vital resources and time frames for restoration of services, facilities and infrastructure.

The following elements should be considered as part of the Recovery plan:

- Strategies to recover critical operations
- Procedures to obtain critical equipment and supplies
- Provisions to accommodate key personnel
- Focus on time-sensitive applications
- Consideration of alternative site resources
- Creation of a special ledger for recording all expenses

Test and implement the plan

After the plan has been drafted, complete a functional exercise and evaluate the essential elements. Use post-incident reports to identify weaknesses and lessons learned, and take corrective action where necessary.

When testing is complete, the plan should be integrated into the operations through the following means:

- Publication (including offsite and web-based access)
- Training, the material to be covered including:
  - cross-training for key personnel
  - details of the emergency action plan
  - evacuation plans
  - alarm systems and reporting procedures for key personnel
  - shut-down procedures
  - types of potential emergencies
- Drills and response rehearsals

Decide on the kind of training needed, who should be trained, and when training should be held. Drills should be organised at random intervals at least annually and should if possible include the police and fire authorities.

Update the plan

After the plan has been implemented and tested satisfactorily, the Planning Team should review the plan to identify, evaluate and update it using the following as a guide:

- Plan components
- Effectiveness and response times
- Discontinuities
- Changes in critical support staff
- Notification information
- Organisational and operational changes
- Impact analyses

Review and update the plan on a regular, at least annual, basis, remaining aware of ways in which you might improve its framework.

Want more information?

National Fire Protection Association (NFPA) 1600, Standard on Disaster/ Emergency Management and Business Continuity Programs

Australian Standard (AS)/New Zealand Standard (NZS) ISO 31000:2009, Risk management – Principles and guidelines

Australian Standard (AS)/New Zealand Standard (NZS) 5050:2010, Business continuity – Managing disruption-related risk

http://www.business.gov.au/business-topics/templates-and-downloads/emergency-management-template-and-guide/Pages/default.aspx

libertyspecialtymarketsap.com

All information in this guide is general in scope and, to the best of our knowledge, current at the time of publication. No attempt has been made to interpret any referenced codes, standards or regulations. You should not rely on this information without first obtaining professional advice. This information is current as at September 2017. Liberty means Liberty Specialty Markets, a trading name of Liberty Mutual Insurance Company, Australia Branch (ABN 61 086 083 605) incorporated in Massachusetts, USA (the liability of members is limited); Liberty Specialty Markets Hong Kong Limited (No. 2400200); and Liberty Specialty Markets Singapore Pte Limited (UEN 201538069C) with a branch in Labuan (Company No. LF12903).