Natural Disaster Contingency Planning

Authors:

Rick Calabrese, Sartorius

Denise Pirko, Boehringer Ingelheim

Dee Ledwin, Daiichi Sankyo

Ken Crossley, Avantor

Norma Amilpa, Eli Lilly

Reviewers:

Leigh Davidson, MilliporeSigma

TABLE OF CONTENTS

SECTION 1: INTRODUCTION

When a natural disaster occurs, oftentimes companies are not adequately prepared to effectively and expeditiously manage the situation to minimize business, customer, and/or patient impact. **Rx-360, an International Pharmaceutical Supply Chain Consortium** has created this Natural Disaster Contingency Planning guideline in response to natural disasters our members are experiencing. This guideline can serve as a baseline to assist your organization to proactively consider how your organization would internally react in the unfortunate circumstance that a natural disaster impacts one of your business locations.

This guideline will address some of the business considerations that your organization may have to address and manage. Preparing and planning ahead of time will allow your organization to more quickly engage and direct the appropriate internal and external (police, fire brigade, disaster response) experts who will be leading your businesses' most critical crisis mitigation activities.

This Natural Disaster Contingency Planning guideline can be used in the event your organization is directly impacted by a natural disaster like a tornado, hurricane, tsunami, blizzard, ice storm, etc. There is a wide range of natural disasters that can happen around the world all with varying levels of risk, severity, and potential impact to your site. This guideline is not inclusive of all the types of natural disasters that can impact your organization, but is being provided to assist you to proactively prepare your organization to immediately transition from impact to recovery if such an event were to occur. Additionally, this guideline can also be referenced in establishing mitigation activities when a natural disaster occurs at one of your global suppliers.

This guideline will assist companies to be cognitive of the impact that a natural disaster could have on your personnel, infrastructure and product/services.

SECTION 2: IMPORTANCE OF PRE-ESTABLISHED PLAN

Companies must prepare themselves if there is a risk of a disaster occurring and this guideline will explain the steps in preparing for contingency plans at your site. Organizations should consider proactively preparing a phased business recovery plan which can be immediately executed when a disaster occurs. A phased business recovery plan including a Disaster Response Plan and a Business Continuity Plan can be employed. The amount of preparation steps that you prepare ahead of time is dependent on the risk and the severity of an event happening at your site and the type of industry.

Depending on the size and complexity of an organization, there may be an overall organization corporate level plan for a disaster as well as more site-specific plans depending on the disasters that have the potential to occur in a given region and the type of activity at each site – like manufacturing vs administrative.

2.1 MINIMIZE RISK TO PERSONNEL

The personnel of an organization are its most important asset. If the personnel are not available to work, then the organization cannot function. Therefore, first and foremost, the organization must develop a plan for evaluating personnel accountability and safety. There must be a complete list of every personnel and several different ways to contact them. In areas where the risk is high of some sort of disaster, the contact list should include additional family or friends in the event the personnel cannot be reached. Provisions must be made to aid personnel to ensure that they and their immediate families are safe and secure. This will allow the personnel to be able to support the organization once they do not have to focus on their own disaster situation. An example of this would be to use an emergency text communication system to contact all personnel.

2.2 MINIMIZE RISK TO FACILITIES

The next most important asset to an organization is the facility where the organization's operations take place. The facility contains all the communication and operational equipment as well as all the documentation and records for the organization. The facility can also contain all the materials and tools used in daily business. Because of this, a disaster plan must be prepared ahead of time to protect these assets as without them the organization cannot function. In the earliest stages, a facility should be built to withstand disasters that have a high risk of occurring in the location of the facility. Redundant systems should also be looked into as warranted by the risk evaluation plan.

2.3 MINIMIZE RISK TO SUPPLY CHAIN/DELIVERY OF SERVICE

A disaster may impact or even halt an organization's ability to provide goods or services. Based on the risk evaluation for the location and type of business, it may be prudent to also develop a business continuity plan to minimize any interruption of the business due to a disaster.
This can include diverting inventory to another location that does not have the same risk of disaster, making arrangements for other locations to provide services, and storing records and documents offsite. Having a plan in place can minimize issues and trying to deal with the situation ad hoc.

The more prepared a location is with a full disaster plan in place prior to a disaster, the more quickly you can then transition to the full business continuity plan, providing for continuation of product and services to maximize a successful return to business.

SECTION 3: EVALUATION OF POTENTIAL RISK

There are two types of risk evaluation that should be performed by all companies. The first type is evaluating the potential for a specific disaster to occur. This information will be used to develop the organization's disaster response plan.

The second type of risk evaluation that should be performed is evaluating the risk to the business as a whole once a disaster strikes. This includes the risk to the delivery of an organization's products or services into the supply chain, as well as the impact on its customers and other interested parties.

3.1 RISK OF DISASTER

The risk of a disaster occurring should be evaluated by an organization in order to be prepared in the event that the disasters do occur. The evaluation should take into account the likelihood of the disaster, the potential for occurrence, and the severity of its impact.

The risk evaluation should start by determining the likelihood of a disaster occurring at the site. This includes identifying the types of disasters that the site can most likely encounter. After making a list of all the potential disasters, the next step would be to determine the potential for them to occur.

There are many resources that can help identify the types of disasters that can occur as well as the potential for them to occur. These resources include national and government websites that post the history of different types of disasters around the world. The insurance provider that covers an organization for casualty and property damage may also be able to provide some useful statistics.

Other factors that can play into the risk evaluation can include, but are not limited to, the design and location of the facility and the type and amount of materials stored within the facility. Although these factors themselves may not lead to a disaster, they can magnify its effect. For example, if the organization has many combustible materials, it can intensify fires. In addition, spilling of hazardous chemicals or biologics can create additional risks for containment.

After the types and potential for a certain disaster have been identified, a disaster response plan can be developed and implemented in the event that a natural disaster occurs.

3.2 RISK TO BUSINESS

The next risk evaluation should be to assess the effect of deterring your products or services from being supplied to your customers or other interested parties. This evaluation should include, but is not limited to, evaluating communication, infrastructure, utility, transportation issues, and the spoilage of product. Other potential risks that should be evaluated may include evaluating the ability for your vendor to deliver materials as well as the ability for them to provide services to repair the damaged facility. There can also be financial risk to the business due to lost revenue or loss of goodwill.

Another risk that needs to be evaluated involves assessing the risk to the customer when there is a disruption in providing products or services to them. The criticality of an organization's products or services will have a substantial impact on the final business risk evaluation.

Multinational companies may choose to create a standard risk evaluation program to simplify the global understanding of the different risks it faces for its business.

Once the risk evaluations of a disaster occurring and the risk to the business have been performed, the organization can than develop the disaster response plan and the business contingency plan for the potential risks associated with the types of disasters for that particular organization. The more critical the products and services are, the more necessary it is for a strategy to be in place to mitigate the risk to keep the business viable.

SECTION 4: PREPARATION OF DISASTER RESPONSE PLAN

A pre-established disaster response plan will allow your organization, and internal and external resources to immediately focus on dealing with the aftermath of the disaster. The disaster plan should include ensuring the safety of your personnel, assuring evacuation procedures are being followed, providing initial disaster response efforts, initiating required damage control, and preparing the contingency plan command center.

4.1 IMPLEMENTATION OF DISASTER COMMAND CENTER

It is important for an organization to establish a Disaster Command Center (DCC) that will carry out the principles of disaster preparedness and disaster management, or disaster management, that functions at a strategic level during a disaster, and ensures the continuity of an organization's operations. The Disaster Command Center should be located in close proximity to the disaster.

An Emergency Command Center (ECC) should be located at the corporation's headquarters and is responsible for strategic direction and operational decisions and does not normally directly control field assets, instead leaving tactical decisions to lower commands. The common functions of ECCs is to collect, gather and analyze data; make decisions that protect life and property, maintain continuity of the organization, within the scope of applicable laws; and disseminate those decisions to all concerned agencies and individuals.

4.2 PERSONNEL DISASTER RESPONSE

Personnel Safety and security
In the event of a disaster, it is important for on-site personnel to first and foremost find safety in a secured location. Personnel should have designated areas to reach safety depending on where the natural disaster impacts the site and its functions. Once personnel are safe, the process for accountability and communication can take place.

Accountability

Personnel accountability is an effort to improve the safety of disaster responders by keeping track of their locations and assignments when operating at an incident site. The timely implementation of personnel accountability processes prohibits a "freelance period" when responders act independent of supervision. Personnel accountability also facilitates the quick identification and removal of injured or incapacitated response personnel from hazardous environments.

Medical Attention

In the event of a disaster, it is important to provide medical attention to personnel that are impacted. It is important to have necessary protocols in place to ensure immediate and appropriate communication to provide medical attention to personnel. The disaster response kit addressed in Section 6.3 will contain items that will help provide medical attention to injured personnel.

Basic Needs

After addressing safety and medical concerns, it is important to attend to the personnel's basic needs. This can include clothing, shelter and food. Each site should address what the potential basic needs could be in event of a disaster.

Crisis Communications Plan

Communication

When a disaster occurs, the need to communicate is immediate and critical. Depending on the severity of the disaster, an organization must be able to communicate with the personnel, families, customers, community, and regulators. Personnel and their families will be concerned and will want information. If business operations are disrupted, customers will want to know how they will be impacted. Neighbors living near the facility may need information—especially if they are threatened by the disaster. Regulators may need to be notified and local government officials will want to know what is going on in their community. All of these "audiences" will want information before the business has a chance to begin communicating.

An important component of the preparedness program is the crisis communications plan. A business must be able to respond promptly, accurately and confidently during a disaster in the hours and days that follow. Many different audiences must be reached with information specific to their interests and needs. The public perception of how an organization handles an incident can positively or negatively impact the image of the business. It is therefore important to have a procedure in place that will be able to communicate the status of the facility and personnel to these audiences. The crisis communication plan will detail the communications between the Emergency Command Center, Disaster Command Center and local and emergency personnel.

Contact Information

Contact information for each audience should be compiled prior to a disaster and be immediately accessible during an incident. Existing information for customers, suppliers, and personnel may be exportable from existing databases. Include as much information for each contact as possible (e.g., organization name, contact name, business telephone number, cell number, fax number and email address).

In addition to having contact information, it is important to have communication methods depending on the severity of the disaster. Information can be communicated to these audiences through a satellite phone system. In cases like this, there should be a designated person (team) in charge of communications.

Management

Management should always be notified no matter what the situation. Protocols for when to notify management should be clearly understood and documented.

Government and Disaster Response

Depending on the severity of the disaster, protocols must be in place to communicate the status of damage to regulators. A designated person should be responsible for this if the event arises.

Personnel, Victims and Their Families

Human Resources (HR) is responsible for the day-to-day communications with personnel regarding employment issues and benefits administration. HR management should assume a similar role on the crisis communications team. HR should coordinate communications with management, supervisors, personnel and families.

The Community

If there are hazards at a facility that could impact the surrounding community, then the community becomes an important audience. If so, community outreach should be part of the crisis communications plan.

- Develop an organization policy where only authorized spokespersons are permitted to speak to the news media on behalf of the organization. Communicate the policy regularly to all personnel explaining that it is best practice to communicate through one informed voice.

- Another important element of the crisis communications plan is the need to coordinate the release of information.

- Another important goal of the crisis communications plan is to move from reacting to the incident, to managing a strategy, to overcoming the incident. Management needs to develop the strategy and the crisis communications team needs to implement that strategy by allaying the concerns of each audience and positioning the organization to emerge from the incident with its reputation intact.

Contact & Information Centers

Communications before, during and following a disaster is bi-directional. Stakeholders or audiences will ask questions and request information. The business will answer questions and provide information. This flow of information should be managed through a communications hub.

4.3 FACILITY DISASTER RESPONSE

The following diagram can be utilized for assessing the appropriate responses when a facility is impacted by a natural disaster. These factors should be evaluated as part of the disaster response plan to ensure continuation of operations.
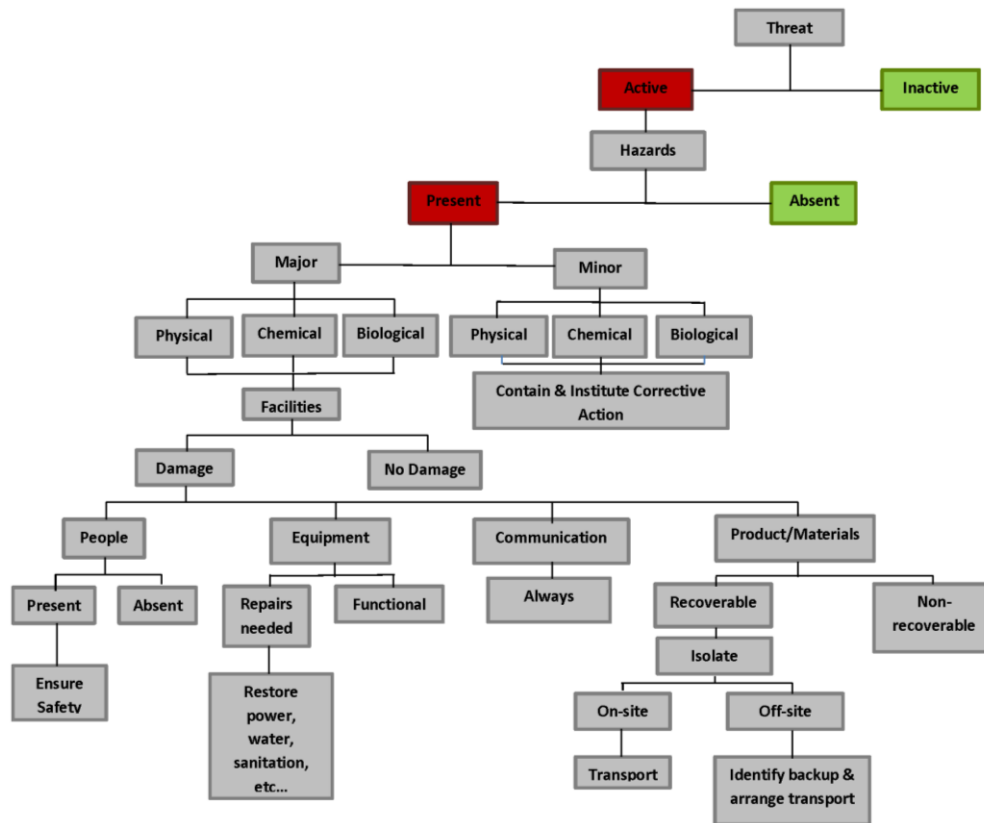
4.4 PRODUCT & SERVICES DISASTER RESPONSE

Individuals of the disaster contingency planning team will assess the impact that the disaster had on in-process and finished products or services. An inventory of the product and the inventory state should be collected. Was the product or services impacted by damage? Does the potential exist for additional damage/risk? If so, plans and actions should be quickly initiated to minimize the potential additional damage / risk?   In this early phase, it may be premature to accurately assess the future disposition of the product into varying classifications: product not impacted, potential sale ability through rework efforts, and full product loss.

In the subsequent days ahead, efforts and personnel can then transition to the evaluation, inspection, segregation, and reworking of any effected product for potential sale. The urgency with these activities will depend on many factors including the supply chain inventory, sole source or multi sourced product or service, customer demands, and infrastructure distribution.

SECTION 5: PREPARATION OF BUSINESS CONTINUITY PLAN

A business continuity plan ensures an organization's ability to continue critical business operational processes in the case of a business interruption. The effective implementation of the business continuity plan is vital to protect the brand and the reputation of the Organization during any unplanned interruption, thus providing a sense of security for its customers and other interested parties.

When business is disrupted, it can cost the organization revenue and sales. A business continuity plan to continue business is essential. Development of a business continuity plan includes four steps:

> **STEP 1:** Conduct a business impact analysis to identify time-sensitive or critical business functions and processes and the resources that support them.

> **STEP 2:** Identify, document, and implement to recover critical business functions and processes.

> **STEP 3:** Organize a business continuity team and compile a plan to manage a business disruption.

> **STEP 4:** Conduct training for the business continuity team and testing and exercises to evaluate recovery strategies and the plan.

Step 1: Business Impact Analysis

Business continuity impact analysis identifies the effects that result as a consequence of disrupting business functions and processes. Business impact analysis also uses information to make decisions about recovery, priorities and strategies.

Those functions or processes with the highest potential for operational and financial impacts become priorities for restoration. The point in time when a function or process must be recovered, before unacceptable consequences could occur, is often referred to as the "Recovery Time Objective."

Step 2: Identify Critical Business Functions

It is important to identify all critical business functions that are necessary to keep the organization operational. This includes all operations that allow the continued delivery of products and services to customers and other interested parties such as, logistics, supply chain, human resources, planning, and sourcing.

This process involves evaluating the sustainability of your product or services to your customers or other interested parties. Is this the only location that manufactures a particular product or provides a particular service? This will play an important role in the development in your business continuity plan.

Step 3: Organize Business Continuity Team

The first step in identifying who needs to be on a Business Continuity Team is to determine what potential events the team will be planning for. Business continuity team should be developed consisting of representatives from different departments that can formulate the short term and long-term strategy to ensure business continuity. The team must develop processes and communication structure to be used in the event of an interruption. The team must also determine the individuals and vendors needed to manage technical recovery.

Teams membership can include but is not limited to:
- Executive Sponsor
- BCM Steering Committee
- Business Continuity Manager
- Key Suppliers and/or retail partners
- Department-Specific Recovery Team Leads:
  - Administration/Risk Management
  - Customer Service

- o Facilities Management
- o Internal/External Communications
- o Manufacturing/Production
- o Information Technology
- o Human Resources
- o Operations/Logistics

Other considerations for developing a recovery strategy should include the following:

- Determine source for back up of technical resources (PCs, servers, printers)
- Document critical data to be restored and back up all data off site.
- Essential tools for virtual continuity management include smart notification and communications systems plus a web-based solution for incident tracking and management that enables all team members have a common operating picture of the incident as it unfolds and access to the files, plans and templates they need to execute their assigned tasks.

Step 4: Business Continuity Training & Evaluation

Training is essential to ensure that everyone knows what to do when there is a disaster, or disruption of business operations. Everyone needs training to become familiar with protective actions for life safety (e.g., evacuation, shelter, shelter-in-place and lockdown). Review protective actions for life safety and conduct evacuation drills ("fire drills") as required by local regulations. Sheltering and lockdown drills should also be conducted. Personnel should receive training to become familiar with safety, building security, information security and other loss prevention programs.

Members of disaster response, business continuity and crisis communications teams should be trained so they are familiar with their role and responsibilities as defined within the plans. Team leaders should receive a higher level of training, including incident command system training, so they can lead their teams. Review applicable regulations to determine training requirements. Records documenting the scope of training, participants, instructor and duration should be maintained.

You should conduct testing and exercises to evaluate the effectiveness of your preparedness program, make sure personnel know what to do and find any missing parts. There are many benefits to testing and exercises:

- Train personnel; clarify roles and responsibilities
- Reinforce knowledge of procedures, facilities, systems and equipment

- Improve individual performance as well as organizational coordination and communications
- Evaluate policies, plans, procedures and the knowledge and skills of team members
- Reveal weaknesses and resource gaps
- Comply with local laws, codes and regulations
- Gain recognition for the disaster management and business continuity program

SECTION 6: EXECUTION OF PREPARED PLANS

When the disaster impacts your organization, a site should immediately activate the pre-established prepared plans and the site Disaster Command Center team. Immediate, organized, and focused response efforts will allow the site management team and personnel to deal with dangerous situations and minimize panic and trauma.

SECTION 6.1: ACTIVATION OF DISASTER COMMAND CENTER TEAM

Immediately upon the onset of a crisis, the Disaster Command Center team will be activated to execute the established prepared plan. The crisis management team will be responsible for managing the personnel to be better equipped in such a situation.

SECTION 6.2: ACCESS TO PLAN/LOCATION OF PLAN

It is critical to have several hard copies of the disaster contingency plan in various locations and with members of the crisis team in the event that electronic IT systems cannot be accessed. Part of the plan should include availability of contact lists for both internal and external resources. It is also recommended to have hard copies of the organization's disaster recovery site procedures which can be accessed.

SECTION 6.3: DISASTER RESPONSE KIT

Organizations should have several pre-prepared disaster response kits that can be immediately deployed to administer disaster care to impacted personnel and/or family members until local disaster response services (medical, fire, utilities) can provide assistance to your site.

Organizations should assess the surrounding facilities, utilizes, and landscape for damage and risk. Your first priority is protecting your personnel from further hazardous and potentially dangerous situations (fire, explosion, collapse, etc.). Building and operations should be contained and deemed safe before allowing routine entry to the areas. Once the facility and surrounding area is stable, an organization should secure the building and product or services to limit future loss.

Since organizations do not know when a disaster will occur or the impact that a disaster can have to a site, it is recommended that organizations have several disaster response kits strategically placed in several locations throughout the facility in the event that any of the disaster response kits are compromised in the disaster. Make sure that all personnel know the locations of the disaster response kits.

The following are items to be considered as part of your site disaster response kits:

Bottled sterile water	Non-Latex Gloves	Two way Radios	Safety Goggles
Flashlights and batteries	Infectious Waste Bags	Satellite cell phones with Wi-Fi	Axe
Spill Clean Up Kit	First Aid Kit including Defibrillator, bandages, compression dressings, adhesive tape, topical ointments, gauze pads and rolls, eye patches, scissors	Duct tape	Tool Kits
Ice packs	Solar blankets	Flares	Caution tape
Hand Sanitizer		Solar Radio	
Disinfectant wipes		Utility Knives	

Throughout the year, review the contents of the disaster response kits and replace expired items as needed. It is also recommended to re-evaluate the contents of the disaster response kit after each mock drill of your site disaster preparedness plan.

SECTION 6.4: COMMUNICATIONS

Organizations should have a pre-established plan for how to account for personnel and how to provide updates and communications to personnel. This is a component of the crisis communications plan. The objectives during a disaster are to account for your personnel, protect your personnel, and ensure personnel are kept informed so that the organization can

survive. It is better to over-communicate than to allow panic, fear, and rumors to fill the void of improper and frequent communications.

The local point of communications should be coordinated through the Crisis Management team at the local command site. The team should predefine who will be providing the communications to the personnel, the frequency at which they will be receiving communications, and in the event that traditional communication modes are not available, what is the plan to get periodic communications to personnel.

SECTION 6.5: DISASTER PLAN CHECKLIST

A copy of the site personnel roster should be part of the disaster response kit and should include cellular phone numbers, addresses, and contact information for an extended family member. The Crisis Management team should manage the accountability for all staff members.

As part of the disaster contingency plan, sites can develop predefined checklist for such things as security of the facilities, access to basic needs provisions, utilities/infrastructure, supply chain, IT systems, disaster contact list (internal and external).

Part of the disaster plan may consider how your personnel will gain access and transportation to the site in the event of a catastrophic disaster including considering carpooling, onsite daycare, flexible scheduling, etc. Assess working remotely if building/transportation is not available.

SECTION 6.6: TRAINING

Conducting training on the disaster contingency plan prior to an event is a critical component to all efficient executed plans. Assuring that individuals are aware of their roles and responsibilities at the site is important to immediately allow for the deployment of your crisis team. It is suggested to hold regular training in crisis management for the Crisis Management Team, which will include practicing mock crisis scenarios and conducting annual practice drills of the evacuation procedure.

As part of the disaster contingency plan, sites can develop predefined checklist for such things as security of the facilities, access to basic needs provisions, utilities/infrastructure, supply chain, IT systems, disaster contact list (internal and external). Disaster recovery training should be part of the on-boarding training of every new personnel.

SECTION 7: EXECUTION OF BUSINESS CONTINUITY PLAN

Once a disaster impacts an organization, the first priority is to enact the disaster response plan for the safety and security of the personnel and the facility where the disaster occurred. It is equally important to initiate the business continuity plan to minimize disruption of products or services to its customers and other interested parties.

There are several actions related to the execution of the business continuity plan

- Ensure that senior management and the corporate owners of the BCP are notified of the disaster as quickly as possible.
- Ensure that the disaster response plan for the facility suffering the disaster has been initiated.
- Communicate to all members of the BCP team that a disaster has struck and the BCP must be initiated
- Ensure that the BCP team is kept apprised of the progress of the disaster response actions for decision making purposes related to the BCP
- Once the BCP has been initiated, internal as well as external communications must be created to inform both personnel, customers and other interested parties
- Finally, it is important to consistently collect information critical to the BCP implementation and adjust response as necessary to minimize the impact to the business operations.

Parallel or separate teams should also be focusing on the restart of operations to offer products and services to your customers or other interested parties. This team will be creating the list of repairs, activities, etc. that must be completed before an organization can be returned to full operation. These steps should also consider any impact or need for re-qualification and/or validation activities and the impact to operation timelines.

SECTION 8 : POST MORTEUM ASSESSMENT

8.1 POST RECOVERY PLAN DEBRIEFING MEETING

Assess the events that took place including the mitigation plans and action by personnel to determine if appropriate plans and procedures were in place, and if they were followed, how effective they were in mitigating the incident.

8.2 SURVEY PERSONNEL AND INTERESTED PARTIES ON RESPONSE ACTIONS

Starting with the detection of the incident, as much information about the incident as possible should be obtained from multiple sources. A checklist of information to be collected and reviewed from each participant aids the process.

8.3 ASSESSMENT*

Things to consider during the assessment:

- Was the Disaster Response Planned followed?
- Was it flexible enough to cope with unexpected events?
- Was the response effective & prompt?

- Reviewing the survey results, identify the strengths in each area, assess the resources mobilized, the ERP and related procedures including the training procedures.

8.4 DOCUMENT ALL ACTIVITES AND MAKE UPDATES TO EXISTING CONTINGENCY PLAN BASED ON FEEDBACK*

The following items should be documented:

- Based on the assessment, document all activities and consider updating the existing contingency plan.

- What changes would have been useful?

- Identified strengths, areas in need of improvement, and make recommendations to better meet plan objectives.

- Track changes to the Contingency Plan and include the rationale for those changes.

*Note these are not all inclusive, it is up to the personnel on site to develop a full and comprehensive list of questions and assessments.

SECTION 9 : CONCLUSION

In our everyday lives no one ever expects an accident to happen, but we take steps to minimize them. Going for a medical checkup, having your car inspected or having a bubble test performed on your barbeque grill propane tanks are all examples of steps to minimize the occurrence of a negative event from taking place. In business operations, and especially within the medical product and service industry, preparing for a potential negative event can be critical not only to the business but also to the end user who may also be a patient.

The first step in being prepared is to understand the disasters which can effect an organization. The next would be to fully understand how this may impact the business. After understanding the related risks, the organization can then prepare both its disaster response plan and its business continuity plan.

The purpose of a Disaster Response Plan is to establish an organizational structure and actions for response to disasters. It assigns the roles and responsibilities for the implementation of the plan during a disaster.

While the business continuity plan is directly related to the disaster response plan, a business continuity plan is a plan to help ensure that business processes can continue during a time of disaster. This includes being able to deliver products and services which may be critical to its customers.

Risk evaluation and development of disaster and business continuity plans are just the first steps. The readiness plans must be fully implemented with any required supplies, materials or adjustments or changes to existing processes or facilities. Personnel then need to be trained on the plans so that it can be effectively executed in times of crisis. This should include auditing the plans for effectiveness and relevance.

As with any project, there should be an evaluation of lessons learned and how the program can be improved upon. A proper Disaster Recovery Plan should help ensure the following critical business considerations:

- People Safety, Security, & Welfare
- Product Safety
- Product Supply
- Critical Infrastructure Capabilities
- Financial / Treasury Responsibilities
- Compliance/Intellectual Property Protection

Finally, no organization ever wants to be subject to a disaster however the amount of resources used to prepare and put together a disaster response plan can pay dividends many times over if the organization is properly prepared for it.

APPENDIX 1: RESOURCES / LINKS

Site	Website
	https://www.eda.gov/files/about/disaster-recovery/biotechnology-pharm-life-sciences.pdf
	http://www.preparemybusiness.org/planning
SBA Disaster Planning	http://www.sba.gov/content/disaster-planning
Federal Disaster Management Agency (FEMA)	http://www.ready.gov/business
Red Cross	http://www.readyrating.org/
Institute for Business and Home Security	http://www.ibhs.org/
Ready	https://www.ready.gov/risk-assessment
Federal Disaster Management Agency	"Every Business should have a plan" (PDF)
	https://www.missionmode.com/readiness-best-practices-assembling-business-continuity-team/
Business Continuity Template	BCP Template 2012(1).docx www.aimnet.org/userfiles/files/BCP%20Template%202012(1).docx
Center for Disease Control (CDC)	Emergency Action Plan Template.doc
	https://www.ready.gov/business/implementation/crisis

APPENDIX 2: DISASTER CHECK LIST 1

Risk	Potential Protective action
Denial of access to facilities	• Continuously update status on social media sites, website, and the press to let customers and personnel know the current status and plans to get running, find temporary space if needed. • Work with local disaster management to participate in any available re-entry programs.
Loss of critical supplier capacity to complete orders	• Establish hard copy and electronic contact lists of primary and alternate suppliers (and competitors). • Establish contingency contracts with alternative suppliers in disparate locations.
Denial of access to key information systems (e.g. Computer systems, databases)	• Establish robust off-site data replication of key information systems and databases • Acquire alternative communication methods to support technology and transaction requirements. • Integrate remote access into operations whenever possible. Ability to work from home for personnel could decrease staffing problems during/after a disaster. • Utilize cloud technology to store critical data remotely.
Lack of communication to suppliers and vendors	• Keep status of business updated on social media and the business' website; inform both suppliers and customers that the business survived the event. Reach out via email blasts. • Reach out to current customers via email blasts and courtesy calls (if possible). If the location is no longer accessible, search for a temporary location nearby and publicize that address. • Consider using more than one telephone provider, again in separate locations • Multiple redundant services and especially proximity of vendors to the area are critical for this cluster.

Vandalism and/or theft	• Develop plans with local law enforcement and disaster management to maintain security during a prolonged absence. • Invest in remotely accessed security and surveillance equipment.
Physical damage	• Develop contact lists of construction contractors, roofers, plumbers, landlords, building management etc. who can reliably respond to physical damage.
Disruption of customers operations	• Develop contact lists of construction contractors, roofers, plumbers, landlords, building management etc. who can reliably respond to physical damage.

APPENDIX 3: DISASTER CHECK LIST 2

1. **Confirm everyone's roles and responsibilities**
   The crisis team determines whether internal or external specialists, or additional internal or external specialists, should be added.

2. **What has happened and what facts have been confirmed?**
   Collect the confirmed facts about the situation. Facts help in deciding what course to adopt.

3. **What assumptions can be made with regard to the incident or situation?**
   Collect the assumptions made so far with regard to the situation. Ensure that these assumptions are examined (action point!) and can be ruled out or are, in fact, the case.

4. **Draw up worst case and most likely scenarios (individually, and make sure to not disregard anything).**
   Handle these in a plenary meeting and keep repeating the following question: what action points have to be observed if these scenarios materialise?

5. **Set priorities (including the LCMT's need for information and necessary instructions and/or tasks for other employees)**
   Consider what information is needed to be able to take decisions. Consider whether other measures are needed which have to be decided on now.

6. **Consider the available and possible options. What has to be done now and what can wait?**
   Consider options for managing the incident and choose the best option.

7. **Set objectives (e.g. return to business as usual).**
   Determine indicators which will enable you to determine whether the outcome of the chosen option is successful.

8. **Identify the stakeholders involved and prioritise according to their interests and any influence they might have.**
   Carry out a thorough analysis of the stakeholders and prioritise according to their interests and influences.

9. **Establish whether stakeholders have to be informed and determine adequate notification for each stakeholder.**
   Determine statements for stakeholders, including the method and times of communication.

10. **Review this protocol every hour.**
    Determine the time and location of the next meeting. Review all steps gone through based on any new information which has become available.

Document Published October 2018.