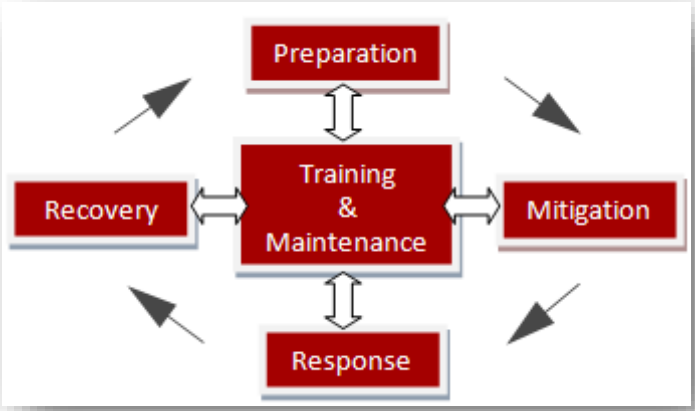
BUSINESS CONTINUITY

PLANNING GUIDELINES

Business Continuity Planning Guidelines
February 2020

BUSINESS CONTINUITY PLANNING

A PRACTICAL APPROACH FOR RC/RC EMERGENCY PREPAREDNESS, CRISIS MANAGEMENT, AND DISASTER RECOVERY



1.0 Introduction

The overall goal of this planning guide is to provide guidance to the Federation Secretariat and Red Cross/Red Crescent Societies about the importance of Business Continuity Planning, which establishes the basis for the organization to continue functioning during the crises, and recover and resume business processes when programs have been disrupted unexpectedly. Because RC/RC societies play a crucial role in the overall emergency disaster response, disruptions in service should be minimized in order to maintain public trust and confidence in the RC/RC emergency response capabilities. As such, RC/RC management should incorporate business continuity considerations into the overall design of their emergency response model to proactively mitigate the risk of program disruptions.

This planning guide is an assembly of existing standard operating procedures, plans and best practises that will explore the key components of a Business Continuity planning process. It will also provide a high-level framework for the creation, implementation, and maintenance of a business Continuity Plan (BCP)..

2.0 Business Continuity Planning Team (BCPT)

Every office of the IFRC Secretariat and possibly every National Society should create a business continuity planning team. As a preeminent organization in disaster preparedness and response, the Federation has an important role to play in emergency response, whether from natural disaster, accidents, or planned actions. By addressing specific concerns and issues inherent to disaster risk management, the Business Continuity Planning Guide will better serve the needs of the Federation Secretariat and RC/RC National Societies by increasing the effectiveness of its programs.

For the specific Coronavirus (2019-nCoV) pandemic preparedness, inside the recently establish coordination cell, a tailored support on BCP is present. All the BCP need to be linked with the contingency plan and the multi hazard preparedness activities aligned with the preparedness for the effective response (PER) concept.

3.0 Scope

The Business Continuity (BC) Planning Guideline is applicable to all IFRC Secretariat office and National Societies and can be adjusted depending on the context of the region and / or the emergency. The BC Guideline is a series of interrelated processes and activities that will assist in creating, testing, and maintaining an organization-wide plan for use in the event of a crisis that threatens the viability and continuity of the RC/RC activities.

PHASE 1 - PREPARATION

Objective:

The first phase of the BCP process is concerned with forward planning (Preparation), to provide a strong foundation on which to build a BCP. At the end of this phase, the following documents will have been created.

Tasks:

1. Assign Accountability

- *Organizational Policy*
- *Business Continuity Planning Team*
- *Delegation of Responsibilities*
- *Communicate BCP*

2. Perform Risk Assessment

- *Risk Management Process*
- *Threats are identified*
- *Vulnerabilities are identified*
- *Risk Assessment*
- *Security Standards*

3. Conduct Business Impact Analysis

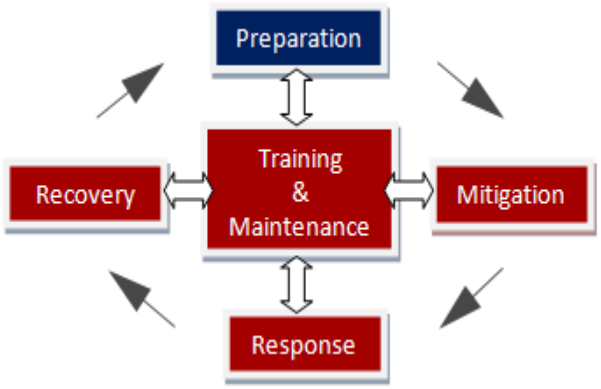
- *Review Types of Risks and the possible Impact on the Organization*

4. Agree on Strategic Plans

- *Identify Critical Processes*
- *Assess Impact if Crisis Were to Happen*
- *Determine Maximum Allowable Down-time and Recovery Time Objectives*
- *Contingency Plans; Relocation and Hibernation*
- *Alternative Sites of Operation*
- *Identify Resources Required for Resumption and Recovery*

5. Crises Management Development

- *Crises management*
- *Crises management team composition*
- *Contact Information*



Assign Accountability

It is the responsibility of the Senior management to support not only the planning process but also the development of the infrastructure to install, maintain, and implement the (BCP). This will ensure that management and staff at all levels within the organization understand that the BCP is a critical top management priority.

Organizational Policy

The senior management should establish policies that define how the organization will manage and control the risks that were identified. In the event of a crisis, an organization wide BCP Policy should be committed to undertaking all reasonable and appropriate steps to protect people, property, and program interests are essential. The policy should include a definition of a ‘‘crisis.’’

Business Continuity Planning Team (BCPT)

Based on the Risk assessment and Business Impact Analysis (BIA), a Business Continuity Planning Team with responsibility for BCP development that includes senior managers from all major departments and volunteer groups should be appointed to ensure wide-spread acceptance of the BCP.

Delegation of Responsibilities

This section should clearly identify the key staff and the delegation of responsibilities for systems, plans, and resources availability. In Appendix C, is the proposed matrix to clearly create and oversee the delegation and responsibilities of tasks. In addition, the plan should specifically identify the key personnel that are needed for successful implementation of the BCP. Plans should assign responsibilities to back-up personnel in the event key employees are not available.

Communicate the BCP

The BCP should be communicated throughout the organization, to ensure all departments are aware of the BCP structure and their roles within the plan.

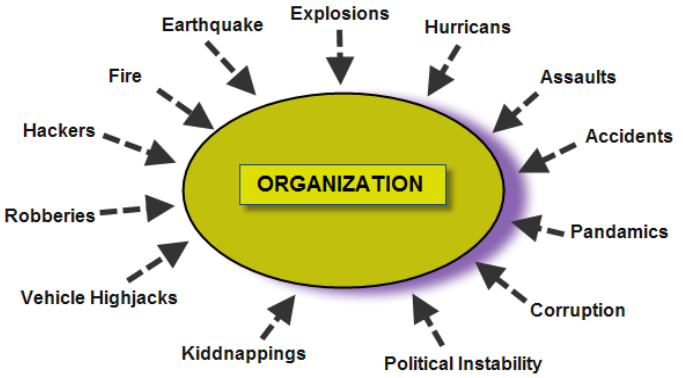
Risk Management Process

The documentation created by this task is the key driver for the determination of the BCP strategy and the creation of the BC plan. In this task, risks are identified, prioritized, and managed; and the overall business impact of the risks is assessed.

In order to create a safer environment, many factors must be considered. The figure below depicts the risk management process, presented to help illustrate the recommended steps for effective risk management.

Threat Assessment

The first step in a risk management program is a threat assessment. A threat assessment considers the full spectrum of threats (i.e., natural, man-made, criminal, militant, accidental, etc.) for a given location. The assessment should examine supporting information to evaluate the likelihood of occurrence for each threat. For natural threats, historical data concerning frequency of occurrence for given natural disasters such as tornadoes, hurricanes, floods, fire, or earthquakes can be used to determine the credibility of the given threat. For criminal threats, the crime rates in the surrounding area provide a good indicator of the type of criminal activity that may threaten the facility. In addition, the type of assets and/or activity your organization is conducting may also increase the target attractiveness in the eyes of the aggressor.



Each RC/RC organization and individual operation will be different. The threats and vulnerabilities will therefore be context-specific, as the risk will also be specific to a particular operation.

Vulnerability Assessment

Once the credible threats are identified, a vulnerability assessment must be performed. The vulnerability assessment considers the potential impact of loss from an incident as well as the vulnerability of the object to an incident. Impact of loss is the degree to which the mission of the organization is impaired by an incident from the given threat.

Having analyzed the threats and vulnerabilities to your staff and organization, the final stage is to assess the risks represented by a combination of these two elements, **threat and vulnerability = risk**

Risk Assessment (RA)

The risk assessment step is critical and has significant bearing on whether business continuity planning efforts will be successful. You've got to understand what's at risk before you can plan to protect it during the risk assessment step, business processes and the Business Impact Analysis (BIA), assumptions are evaluated using various threat scenarios. The RA should be performed by a group representing various organizational functions and support groups. There are various methodologies for the creation of a risk assessment module, the preferred approach by the Federation Security Unit can be found in the 'Stay Safe Guide for Managers' and in the FedNet under Security, available at; https://fednet.ifrc.org/en/resources/security/

A useful tool for assessing risk is a risk-planning matrix, which is illustrated on the next page and which is available as a template in an electronic format on FedNet or from the regional Security Coordinator and/or the Security Unit in Geneva. This requires that various threat scenarios be plotted on the matrix according to their likelihood of occurring. The potential impact they may have is clearly determined by the vulnerability of the operation. From this, we can assess the level of risk that the various scenarios present, ranging from low to extreme.

Security Standards

Security standards should be an integral part of the entire business continuity planning process. During a disaster, security becomes very important due to potential changes in the working environment, personnel, and equipment. Consequently, different security risks will emerge that should be considered during the risk assessment process. Ultimately, mitigating strategies should incorporate the various risks identified to ensure that adequate security controls are in place if an event triggers the implementation of the BCP. Additionally, security standards should be incorporated into the BCP training and testing program.

Conduct Business Impact Analysis (BIA)

Review Types of Risks that could Impact the Business

Using available information about known or anticipated risks, the organization should secure its business and critical infrastructure, whether from natural or man-made disasters, accidents, or planned actions. The critical process is to identify and review risks that could possibly impact the business and rate the likelihood and impact of each. A Risk Assessment matrix can aid identification of risks and prioritization of mitigation/planning strategies.

Once the risks have been identified and plotted in the Risk Matrix, a Business Impact Analysis (BIA) can be made. The BIA is an integral component of the overall BCP. A key aim of the BCP must be to reduce or to mitigate the risk to an acceptable level for the continuity of the business. From the matrix, it should be obvious that this can only be done by reducing the likelihood and/or by reducing the impact.

Impact Level

Likelihood

	negligible	minor	moderate	severe	critical
Frequent/ Imminent					
Probable					
Occasionally					
Remote					
Unlikely					

	Extreme risk: Undesirable, immediate action required - Can it be mitigated? If so how? and it must be tested and rehearsed.
	High risk: Undesirable, priority action - Contingency plans developed and tested.
	Moderate risk: Requires heightened awareness and specific procedures.
	Low risk: Managed by routine procedures.

The BIA can be adjusted to cover any specific requirement from natural or man-made disasters, security concerns to pandemic outbreaks. The purpose is to identify the effect of many different external and internal impacts upon the various parts of your organization in times of crisis. It will show which parts of your organization will be most affected by an incident and what effect it will have upon the organization as a whole. In other words, we will use the BIA to establish the most critical business functions to your organization's survival.

Each Red Cross/Red Crescent society is unique and can have from a few to hundreds of programs in its overall business but only a segment of these will be key to its survival and it is these that we need to build business contingencies for. Of course, we will not ignore the remainder but because they are less critical, we can prepare recovery plans for them instead.

Agree on Strategic Plans

The business continuity strategy represents a critical aspect of the BCP and is derived from the information collected during the risk assessment and the business impact analysis (BIA) process. The following components should be considered when defining the business continuity strategy and developing the BCP. An organizational-wide BCP may include multiple strategies that address a variety of probable crises.

Identify the critical aspects of an organization

This step determines the critical aspects for the continuation of the programs. They could include Admin, HR, finance, logistics, IT, etc. Once the critical aspects are identified, an analysis of each can be made using the evaluation criteria described below.

Assess Impact if Crisis Were to Happen

- *Human cost:* physical and psychological harm to delegates, family members, consultants, visitors, NS partners, volunteers, other stakeholders, etc.
- *Financial cost:* equipment and property replacement, overtime pay, contract penalties.
- *Organizational image cost:* reputation, standing in the community, RC/RC partners, volunteers, negative press, affected population

Determine Maximum Downtime

The BIA should estimate the maximum allowable downtime for critical business functions and processes and the acceptable level of losses (data, operations, financial, and reputation), associated with this estimated downtime.

- Determine how long your office and programs can be non-functional before impacts become unacceptable
- Determine how soon your office and programs can be restored

Contingency Plans

Contingency plans provide an outline of decisions and measures to be taken if circumstances should occur in relation to a specific activity. Contingency plans generally relate to a planned event, while the business continuity plans relate to programs and assets that are already operational. Contingency plans can include a variety of situations, all depending on the results from the risk assessment. The plans can include but not limited to, fire response, medical evacuation, vehicle accidents, relocation and hibernation plans. Even though the risks are different, the development of the contingency plan is relatively uniformed.

- set priorities and goals
- identify activities and tasks
- allocate resources
- allocate responsibilities
- set order of implementation
- ensure technical inputs
- develop procedures

Alternative Sites of Operation

In the event of serious damage to, or exclusion from key premises, the organization would have an urgent need for specific, predetermined alternative office site facilities in order to establish continuity of critical program functionality, even in a reduced form. These, together with re-established computer systems and back-up data likely required within one working day to ensure adequate continuity.

For more information concerning contingency planning, use the following link: https://www.ifrc.org/en/what-we-do/disaster-management/preparing-for-disaster/disaster-preparedness-tools/contingency-planning-and-disaster-response-planning/

Identify Resources Required for Resumption and Recovery

Such resources can include personnel, technology hardware and software (including Telecommunications), specialized equipment, general office supplies, facility/office space and critical business records. Identifying, backing-up, cloud services and storing critical and vital business records in a safe and accessible location are essential prerequisites for an effective BCP.

Crises Management Development

Crises management

A crises management team is to be set up once the details of the incident have been confirmed. From the moment a crisis is confirmed, the crisis management team takes over all line management and operational responsibilities for the incident. The lines of command should be as short as possible and the authority of the team sufficiently strong to allow immediate, urgent decisions to be made; but also equally restrained as far as the potential liability of the organization as a whole is concerned.

A crises is defined as a situation that threatens – or has impacted on – the safety or security of Federation personnel, assets or operations to the extent that there is likely to be a significant disruption – or even inability – to continue to operate within the country and which may require support from Geneva-based Federation assets to address the impact.

As this process is worked though, it is important to gather as much relevant information as quickly as possible. This, in turn, enables a decision to be made as to whether this is a simple incident and can be managed according to normal procedures, or whether this is a critical incident and will, therefore, need to be managed as such.
Regardless of the level of critical incident, there is a series of stages that must be completed:

1. Establishing what happened
2. Analyzing the situation
3. Option analysis
4. Implementation
5. Follow-up

Crises management team composition

Ideally, the crises management team should comprise between three and five experienced staff from the key departments involved. One person from the group should be appointed Critical Incident Manager (CIM).

Others may be seconded for specific planning or execution tasks. It is vital, however, that the team does not get too big and become ineffective in planning and making decisions. Members of the critical incident management team are only there because they have specific technical expertise to contribute.

Although policies will not always cover every eventuality, having contingency plans and regularly updating them to work through ‘what if?’ scenarios, as well as having effective crisis management procedures in place, will go a long way towards keeping a situation under control and maintaining safe operations.

For more information concerning the Federations Critical Incident Management Protocol go to FedNet, and use the following link:
https://fednet.ifrc.org/en/resources/security/security-management/

Contact Information

Contact information for personnel assigned to crisis management should be included in the plans. Personal information such as unlisted phone numbers and home addresses should be protected. The organization should establish procedures to ensure that the information is kept up to date.

MITIGATION

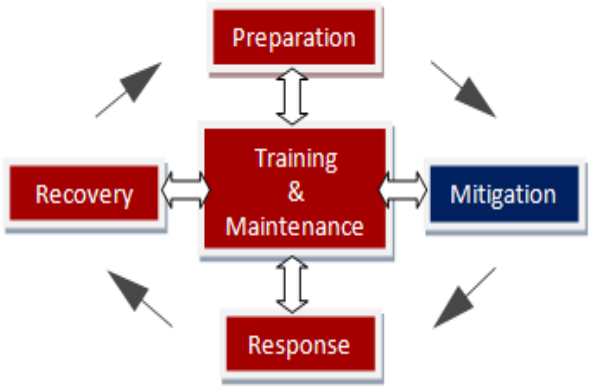
Objective:

Management should develop comprehensive mitigation strategies to resolve potential problems that may result from internal and external interdependencies. Mitigation strategies will depend upon the results of the BIA and risk assessment but should always ensure that processing priorities can be adequately implemented and that business operations can be resumed in a timely manner.

Tasks:

Mitigation Strategies

Devise Mitigation Strategies.



Mitigation Strategies

Devise Mitigation Strategies

Cost effective mitigation strategies should be employed to prevent or lessen the impact of potential crises. For example, securing equipment to walls or desks with strapping can mitigate damage from an earthquake; sprinkler systems can lessen the risk of a fire; a strong records management and technology disaster recovery program can mitigate the loss of key documents and data.

If a pandemic occurs, you may be able to mitigate the impact on your organization by creating a working atmosphere that promotes health - and aims to reduce the potential spread of the virus among your employees. Creating a healthy workplace, could include the identification of office infectious control measures (clean and “dirty” zones) and movement of the staff coming and leaving the office.

Resources Needed for Mitigation

The following represent examples of appropriate mitigation strategies:

- Strengthening the physical facility using dependable construction materials;
- Establishing media protection safeguards and comprehensive data back-up procedures;
- Implementing redundant or alternative power sources, communication links, data back-up technologies, and data recovery methods;
- Procuring inventories of critical equipment; medicine stocks, protective gear, etc.
- Installing fire detection and suppression systems.
- Purchasing and maintaining adequate reserves of food, water, batteries, and medical supplies.
- Fire alarms and suppression systems
- Protective wear, health masks, gloves, suites, etc.

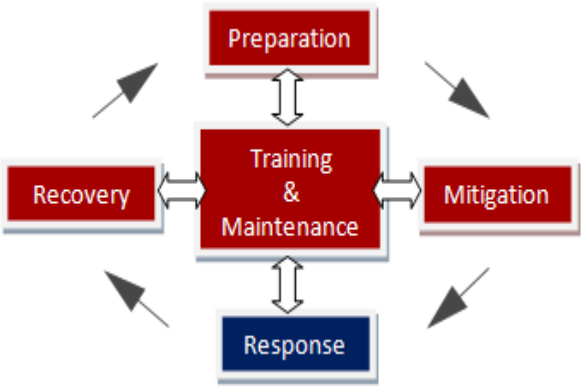
RESPONSE

Objective:

This section includes the reactive part of the planning process. This incorporates ideas and strategies for dealing with the impacts - at both organizational and operational levels. Understand and document your options, then put them into action as needed when the situation requires.

Tasks:

1. Declare the Crises
2. Execute the Plan
3. Create Communication Plan
4. Resources Management



Declare a Crisis

The point at which a situation is declared to be a crisis should be clearly defined, documented, and fit very specific and controlled parameters. Responsibility for declaring a crisis should also be clearly defined and assigned. First and second alternates to the responsible individual should be identified.

The activities that declaring a crisis will trigger various contingency plans; include, but are not limited to:

- Additional call notification
- Evacuation, hibernation, or relocation
- Safety protocol
- Response site and alternate site activation
- Team deployment
- Personnel assignments and accessibility
- Emergency contract activation
- Operational changes.

In certain situations, there may be steps that can and should be implemented, even without officially declaring a crisis.

Emergency Phase System

These levels may aid organizations that are developing response plans and implementation ‘‘triggers’’ for use during a crisis. Determining the initial level of the crisis and the progression from one level to the next will normally be the responsibility of the Crisis Management Team.

The Federation operates a four-color phase system to distinguish the situation

White phase	Situation normal	No major security/health concerns
Yellow phase	Situation of heightened tension	**Limited impact** on the Business Continuity. • Some security/health concerns. • Heightened security awareness initiated. • Local media only
Orange phase	Emergency situation	**Moderate Impact** on Business Continuity • Risk to Red Cross Red Crescent personnel severe, • Tight security management needed • Several injuries or deaths • Moderate damage • Moderate community impact • Access to beneficiaries limited. • National/International media
Red phase	Relocation or hibernation	**Major Impact** on Business Continuity • Major Impact on all areas • Conditions do not allow work, risk to Red Cross Red Crescent personnel extreme

- All staff must know the current security phase classification and it's implication on the way of working and living in their area of operation or area that will be visiting.
- All staff is to comply with any restrictions put in place by the senior management in accordance with the current situation and designated phase level.

Emergency Procedures

All personnel must know their place and tasks in an emergency situation and be aware of the security implications it will have in their A.O. RC Personnel must also be familiar with their role and responsibilities in the BCP and Relocation Plan. See separate attachment – BC Planning Matrix: Delegation of Responsibilities & Assignments

Execute the Plan

BCPs should be developed around a ''worst case scenario,'' with the understanding that the Response can be scaled appropriately to match the actual crisis in accordance with the Federation emergency phase system. When initiating a response, it is important to ensure that the goals protect the following interests listed in order of their priority:

- Save lives and reduce chances of further injuries/deaths
- Uphold and protect human dignity

- Protect assets
- Restore critical business processes and systems
- Reduce the length of the interruption of business
- Protect reputation damage
- Control media coverage (e.g. local, regional, national or global)
- Maintain donor relations.

Communications

Communication is the key in any crises – this section should define the internal and external audiences and the types of communication equipment needed.

Identify the Players

Internal and external audiences should be identified in order to convey crisis and organizational response information. In order to provide the best communications and suitable messages for various groups, it is often appropriate to segment the audiences. In this way, messages tailored specifically for a group can be released.

Internal	External
• Staff and their families • Partners • Consultants, Visitors • Onsite Contractors	• Affected Population • Contractors • Media • Government and Regulatory Agencies • Local law enforcement • Emergency responders • Surrounding communities

Communicating with Audiences

The following items should be taken into account in the crisis communications strategy:

- Communications should be timely and honest.
- To the extent possible, an audience should hear news from the organization first.
- Communications should provide objective and subjective assessments.
- All employees should be informed at approximately the same time.
- Give bad news all at once – do not sugar-coat it.
- Provide opportunity for audiences to ask questions, if possible.
- Provide regular updates and let audiences know when the next update will be issued.
- Treat audiences as you would like to be treated.
- Communicate in a manner appropriate to circumstances:
    - _ Face-to-face meetings (individual and group)
    - _ News conferences
    - _ Voice mail/email
    - _Company Intranet and Internet sites
    - _ Special newsletter
    - _ Announcements using local/national media.

Official Spokesperson

The organization should designate a single primary spokesperson, with back-ups identified, who will manage/disseminate crisis communications to the media and others. This individual should be trained in media relations prior to a crisis. All information should be channelled through a single source to assure that the messages being delivered are consistent. It should be stressed that personnel should be informed quickly regarding where to refer calls from the media and that only

authorized spokespeople are to speak to the media. In some situations, an appropriately trained site spokesperson may also be necessary.

Resource Management

Before, during and after a crisis, the management of the Human Resource aspect is of vital importance, for the continuity of the business. Consider that mentally healthy employees are more likely to be effective in the workplace. Below is a list of issues that need to be considered.

The Human Element

People are the most important aspect of any BCP. How an organization's human resources are managed will impact the success or failure of crisis management.

Manage Skill Sets

Conduct a thorough census of your Employee base

- Identify individuals with particular skill sets.
- Identify individuals with particular functional experience.
- Identify individuals with other similar capabilities.

Accounting for All Individuals

A system should be devised by which all personnel can be accounted for quickly after the onset of a crisis. This system could range from a simple telephone tree. Current and accurate contact information should be maintained for all personnel.

Notification of Next-of-Kin

Arrangements should be made for notification of any next-of-kin in case of injuries or fatalities. If at all possible, notification should take place in person by a member of senior management.

Crisis Counselling

Crisis counselling should be arranged as necessary. In many cases, such counselling goes beyond the qualifications and experience of an organization's HR capabilities. Other reliable sources of counselling should be identified prior to a crisis situation.

Financial Support

A crisis may have far reaching financial implications for the organization, its employees and their families, and other stakeholders; these implications should be considered an important part of a BCP. Implications may include financial support to families of victims. Additionally, there may be tax implications that should be referenced and clarified in advance.

Salaries

The salary system should remain functional throughout the crisis.

Infrastructure

Logistical decisions made in advance will impact the success or failure of a good BCP. Among them are the following:

Emergency Operations Centre (EOC)

In typical "crisis" management planning, an EOC is intended to provide an alternate command centre - a place from which to manage the situation if the existing premises are damaged, unavailable or not suitable. The site should have an uninterruptible power supply, essential computer, telecommunications, heating/ventilating/air conditioning systems, and other support systems. Additionally, emergency supplies should be identified and kept in the EOC. Where a dedicated EOC is not possible, a designated place where the Teams may direct and oversee crisis management

activities should be guaranteed. A secondary EOC should also be identified in the event that the primary Centre is impacted by the crisis event.

Offsite Storage

Offsite storage is a valuable mitigation strategy allowing rapid crisis response and business Recovery/resumption. The off-site storage location should be a sufficient distance from the primary facility so that it is not likely to be similarly affected by the same event. Items to be considered for off-site storage include critical and vital records (paper and other media) necessary to the operations of the business. Procedures should be included in the plan to ensure the timely delivery of any necessary items from offsite storage to the Emergency Operations Centre or the alternate worksites.

Financial Issues and Insurance

If appropriate, existing funding and insurance policies should be examined, and additional funding and insurance coverage should be identified and obtained. Policy parameters should be established in advance, including pre-approval by the insurance provider of any response related vendors. Where possible, the amount of funds to help ensure continuity of operations should be determined in the planning process. Additionally, any cash should be stored in an easily accessible location to assure its availability during a crisis. Some cash and credit should also available for weekend and after-hours requirements.

All crisis related expenses should be recorded throughout the response and recovery/ resumption periods.

Insurance providers should be contacted as early as possible in the crisis period, particularly in instances of a wide-reaching crisis, where competition for such resources could be vigorous. All insurance policy and contact information should be readily available to the Crisis Management Team and backed up or stored offsite as appropriate.

Suppliers Providers

Once all critical supplies (raw materials, water, food, office supplies, etc.) have been identified in the Impact Analysis, decisions should be made regarding the stockpiling of "mission-critical" supplies (those without which the business cannot function) in the event suppliers (or the marketplace) cannot continue to provide the quantities needed during the emergency.

- Stockpile - keep a longer-lasting supply of essential goods on hand.
- Disperse geographically - diversify to help ensure availability.
- Understand transportation alternatives - and be prepared to use them.

Transportation

What alternatives are available if your "normal" means of supply and delivery transportation are reduced or impaired? Consider not only how Suppliers will get their materials to you - but how you will deliver to your beneficiaries. Provisions should be arranged ahead of time, if possible. Areas where transportation is critical include, but are not limited to:

- Evacuation of personnel (e.g., from a demolished worksite or from a field office in another country)
- Transportation to an alternate worksite
- Supplies into the site or to an alternate site
- Transportation of critical data to worksite
- Transportation for staff with special needs.

Mutual Aid Agreements

Mutual aid agreements identify resources that may be borrowed from other organizations during a crisis, as well as mutual support that may be shared with other organizations. Such agreements should be legally sound and properly documented, clearly understood by all parties involved, and representative of dependable resources as well as a commitment to cooperation.

RECOVERY

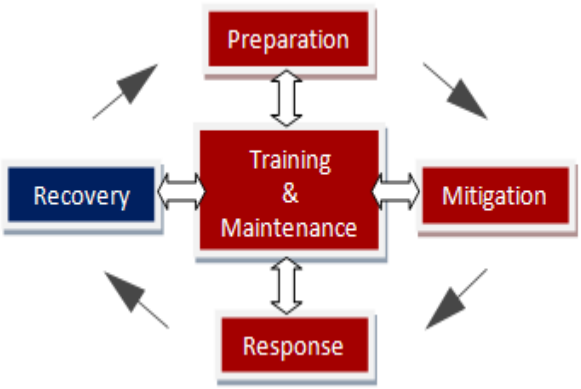
Objectivity,
When it's over, a formal process for returning to "normal" will help anticipate needs - as well as gain insight (about your business, your suppliers, your beneficiaries and your staff) from the experience.

Tasks:

1. Damage & Impact Assessment

2. Resumption of Critical & Remaining Processes
   - *Process Resumption Prioritization*
   - *Resumption of Critical Processes*

3. Return to Normal Operations
   - *Review and Follow-up*



Damage and Impact Assessment

Once the Crisis Management Team has been activated, the damage should be assessed. The damage assessment may be performed by the Crisis Management Team itself or a designated Damage Assessment Team. Responsibility should be assigned for the documentation of all incident related facts and response actions, including financial expenditures.

Resumption of Critical and Remaining Processes

Process Resumption Prioritization

It is unlikely that anyone will sound the "All Clear" bell when the crisis is over. More likely, return to a "normal" state will happen slowly, and with varying degrees of subtlety. The new "normal" may not be like the pre-crises "normal". You should take steps to assess your situation carefully - both to be certain the risk of spread has passed, and to determine what your organization can and should do to get back to business.

You may want to consider reassessing the impact of the crisis on your organization by performing an update of your BIA or process models. Or you may simply want to find the quickest and easiest way to get back up and running. Regardless, you will need to spend some time addressing important issues such as:

- Business assessment
- Supplier availability
- Relationship to the affected populationStaff assistance
- Clearing backlogs
- Debriefing to learn from your experiences

Resumption of Critical Processes

Assuming the impact of the crisis has passed, what do you do now?

It may not be possible (or prudent) to return to "normal". Assess your situation first.

- Has the context for your programs changed? Is it permanent or temporary? How long?
- Has the beneficiary base changed? Do you need to rethink your programs strategies?
- Have suppliers changed? Will new relationships continue? Can/should old ones be revived?

Return to Normal Operations

In the post-crisis phase, the organization is returning to business as usual. The crisis is no longer the focal point of management's attention but still requires some attention, including follow-up communication that is required. The organization will also need to release updates on the recovery process, corrective actions, and/or investigations of the crisis. The amount of follow-up communication required depends on the amount of information promised during the crisis and the length of time it takes to complete the recovery process.

Review/follow-up

After the incident has been resolved, a debriefing process should be implemented. The debriefing process should work through the incident from start to finish and examine actions taken at each stage. Lessons learnt should be identified and recorded, while any required changes to existing procedures and regulations should be implemented without delay. It is also important to assign actions for follow-up requirements such as personnel counselling, legal proceedings, insurance claims, etc.

TRAINING & MAINTENANCE

Objective; Training / Maintenance

This section of the guideline contains those functions and tasks required for the Business Continuity Plan to remain a living document: one that grows and changes with the organization and remains relevant and actionable. Train and educate team members, validate and enhance the BCP.

Tasks:

1. Educate & Train
   - *Educate and Train Teams*
   - *Educate and Train All Personnel*

2. **Develop BCP Review Schedule**

3. **Develop BCP Maintenance Schedule**

Educate and Train

The BCP is only as valuable as the knowledge that others have of it. Education and training are necessary components of the BCP process. They require a time commitment from the Crisis Management Team, the Response Teams, and the general employee population.

Educate and Train Teams

The Crisis Management Teams should be educated about their responsibilities and duties. Check lists of critical actions and information to be gathered are valuable tools in the education and response processes. Teams should be trained at least annually, and new members should be trained when they join.

Educate and Train All Personnel

All personnel should be trained to perform their individual responsibilities in case of a crisis. They should also be briefed on the key components of the BCP, as well as the Response Plans that affect them directly. Such training could include procedures for evacuation, shelter-in-place, check-in processes to account for employees, arrangements at alternate worksites, and the handling of media inquiries by the company.

Develop BCP Review Schedule

The BCP should be regularly reviewed and evaluated. Reviews should occur according to a pre-determined schedule and documentation of the review should be maintained as necessary. The following factors can trigger a review and should otherwise be examined once a review is scheduled.

Risk Assessment

The BCP should be reviewed every time a risk assessment is completed for the organization. The results of the risk assessment can be used to determine whether the BCP continues to adequately address the risks facing the organization.

Event Experience

A review should be performed following a response to an event, whether the BCP was activated or not. If the plan was activated, the review should take into account the history of the plan itself, how it worked, why it was activated, etc. If the plan was not activated, the review should examine why and whether this was an appropriate decision.

Test/Exercise Results

Based on test/exercise results, the BCP should be modified as necessary.

Develop BCP Maintenance Schedule

Regular maintenance of the BCP cannot be overemphasized. Clear responsibility for BCP maintenance should be assigned. Maintenance can be either planned or unplanned and should reflect changes in the operation of the organization that will affect the BCP. The following are examples of procedures, systems, or processes that may affect the plan:

- Systems and application software changes
- Changes to the organization and its business processes
- Personnel changes (employees and contractors)
- Supplier changes
- Critical lessons learned from testing
- Issues discovered during actual implementation of the plan in a crisis
- Changes to external environment (new threats in the area, political changes, infrastructure changes, etc.)
- Other items noted during review of the plan and identified during the Risk Assessment.

13.0 REFERENCES/BIBLIOGRAPHY

American Red Cross. *Preparing Your Business for the Unthinkable*. Washington, DC: www.redcross.org

Global Disaster preparedness centre (GDPC) - Business preparedness Initiative https://www.preparecenter.org/activities/business-preparedness-initiative

WHO Pandemic preparedness https://www.who.int/influenza/preparedness/pandemic/en/

Appendix A

Alternate Worksite– A work location, other than the primary location, to be used when the primary location is not accessible.

Business Continuity– A comprehensive managed effort to prioritize key business processes, identify significant threats to normal operation, and plan mitigation (response) strategies to ensure effective and efficient organizational response to the challenges that surface during and after a crisis.

Business Continuity Plan (BCP)– An ongoing process supported by senior management and funded to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure the continuity of operations through personnel training, plan testing, and maintenance.

Business Impact Analysis (BIA) – A management level financial analysis that identifies the impacts of losing an organization's resources. The analysis measures the effect of resource loss and escalating losses over time in order to provide reliable data upon which to base decisions on mitigation, recovery, and business continuity strategies.

Contact List– A list of team members and key players in a crisis. The list should include home phone numbers, pager numbers, cell phone numbers, etc.

Crisis– Any global, regional, or local natural or human-caused event or business interruption that runs the risk of (1) escalating in intensity, (2) adversely impacting shareholder value or the organization's financial position, (3) causing harm to people or damage to property or the environment, (4) falling under close media or government scrutiny, (5) interfering with normal operations and wasting significant management time and/or financial resources, (6) adversely affecting employee morale, or (7) jeopardizing the organization's reputation, products, or officers, and therefore negatively impacting its future.

Critical Incident Manager - The CIM is responsible for assembling the Critical Incident Management Team (CIMT) and then managing the response to the situation and is relieved from the responsibilities of their regular position for the duration of the response.

Crisis Management– Intervention and coordination by individuals or teams before, during, and after an event to resolve the crisis, minimize loss, and otherwise protect the organization.

Crisis Management Center– A specific room or facility staffed by personnel charged with commanding, controlling, and coordinating the use of resources and personnel in response to a crisis.

Crisis Management Team– A group directed by senior management or its representatives to lead incident/event response comprised of personnel from such functions as human resources, information technology facilities, security, legal, communications/media relations, manufacturing, warehousing, and other business critical support functions.

Critical Function– Program activity or process that cannot be interrupted or unavailable for several working days without having a significant negative impact on the organization.

Critical Records– Records or documents that, if damaged, destroyed, or lost, would cause considerable inconvenience to the organization and/or would require replacement or recreation at a considerable expense to the organization.

Damage Assessment– The process used to appraise or determine the number of injuries and human loss, damage to public and private property, and the status of key facilities and services resulting from a natural or human-caused disaster or emergency.

Disaster– An unanticipated incident or event, including natural catastrophes, technological accidents, or human-caused events, causing widespread destruction, loss, or distress to an organization that may result in significant property damage, multiple injuries, or deaths.

Disaster Recovery– Immediate intervention taken by an organization to minimize further losses brought on by a disaster and to begin the process of recovery, including activities and programs designed to restore critical business functions and return the organization to an acceptable condition.

Emergency– An unforeseen incident or event that happens unexpectedly and demands immediate action and intervention to minimize potential losses to people, property, or profitability.
Evacuation– Organized, phased, and supervised dispersal of people from dangerous or potentially dangerous areas.
Evaluation and Maintenance– Process by which a business continuity plan is reviewed in accordance with a predetermined schedule and modified in light of such factors as new legal or regulatory requirements, changes to external environments, technological changes, test/exercise results, personnel changes, etc.
Exercise– An activity performed for the purpose of training and conditioning team members and personnel in appropriate crisis responses with the goal of achieving maximum performance.
Mitigation Strategies– Implementation of measures to lessen or eliminate the occurrence or impact of a crisis.
Mutual Aid Agreement– A pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement.
Prevention– Plans and processes that will allow an organization to avoid, preclude, or limit the impact of a crisis occurring.
Readiness– The first step of a business continuity plan that addresses assigning accountability for the plan, conducting a risk assessment and a business impact analysis, agreeing on strategies to meet the needs identified in the risk assessment and business impact analysis, and forming Crisis Management and any other appropriate response teams.
Recovery/Resumption– Plans and processes to bring an organization out of a crisis that resulted in an interruption. Recovery/resumption steps should include damage and impact assessments, prioritization of critical processes to be resumed, and the return to normal operations or to reconstitute operations to a new condition.
Response– Executing the plan and resources identified to perform those duties and services to preserve and protect life and property as well as provide services to the surviving population. Response steps should include potential crisis recognition, notification, situation assessment, and crisis declaration, plan execution, communications, and resource management.
Risk Assessment– Process of identifying internal and external threats and vulnerabilities, identifying the likelihood of an event arising from such threats or vulnerabilities, defining the critical functions necessary to continue an organization's operations, defining the controls in place or necessary to reduce exposure, and evaluating the cost for such controls.
Shelter-in-Place– The process of securing and protecting people and assets in the general area in which a crisis occurs.
Simulation Exercise– A test in which participants perform some or all of the actions they would take in the event of plan activation. Simulation exercises are performed under conditions as close as practicable to ''real world'' conditions.
Tabletop Exercise– A test method that presents a limited simulation of a crisis scenario in a narrative format in which participants review and discuss, not perform, the policy, methods, procedures, coordination, and resource assignments associated with plan
activation.
Testing– Activities performed to evaluate the effectiveness or capabilities of a plan relative to specified objectives or measurement criteria. Testing usually involves exercises designed to keep teams and employees effective in their duties and to reveal weaknesses in the Business Continuity Plan.
Training– An educational process by which teams and employees are made qualified and proficient about their roles and responsibilities in implementing a Business Continuity Plan.
Vital Records– Records or documents, for legal, regulatory, or operational purposes, that if irretrievably damaged, destroyed, or lost, would materially impair the organization's ability to continue business operations.

APPENDIX B

	Business Continuity Guideline Checklist	Y/N	Notes
	Considerations		
1	If a major disaster occurred today, has your organization planned for survival?		
2	Does your organization have a Business Continuity Plan (BCP), and is it up to date?		
3	Has senior management approved the BCP?		
4	Does senior management support the BCP?		
5	Has the cost of the BCP been determined, including development and maintenance?		
6	Have the initial audit, security, and insurance departments reviewed the BCP?		
7	Has the BCP been tested, including a surprise test?		
	DEVELOPING THE PLAN **Accountability**		
1	Does your organization's policy include a definition of crisis?		
2	Has the person responsible for critical systems and business processes been identified?		
3	Has a BCP Team been appointed, and does it include senior business function leaders?		
4	Has the BCP been communicated throughout the organization?		
5	Has a person been assigned with the responsibility to update the BCP?		
	DEVELOPING THE PLAN **Risk Assessment**		
1	Has your organization conducted a Risk Assessment?		
2	Have the types of risks that may impact your organization been identified and analyzed?		
3	Has the likelihood for each type of risk been rated?		
	DEVELOPING THE PLAN **Business Impact Analysis**		
1	Have the critical business processes been identified?		
2	If a crisis were to happen, has the impact, in terms of human and financial costs, been assessed?		
3	Have the maximum allowable outage and recovery time objectives been determined?		
4	Has the length of time your organization's business processes could be non-functional been determined?		
5	Have the recovery time objectives been identified?		
6	Have the resources required for resumption and recovery been identified?		
	DEVELOPING THE PLAN **Strategic Plans**		
1	Have methods to mitigate the risks identified in the Business Impact		

	Analysis and Risk Assessment been identified?		
2	Have plans and procedures to respond to any incident been developed?		
3	Have strategies that address short- and long-term business interruptions been selected?		
4	Are the strategies attainable, tested, and cost effective?		
	DEVELOPING THE PLAN **Crisis Management and Response Team Development**		
1	Is the Crisis Management Team comprised of members from human resources?		
2	Have response plans to address the various aspects of the crisis been developed and incorporated into the organization's overall BCP?		
3	Do the response plans address damage assessment, site restoration, payroll, human resources, information technology, and administrative support?		
4	Has contact information been included in the plan for the Crisis Management and the Response Teams?		
	PREVENTION **Compliance w/Corporate Policy & Mitigation Strategies**		
1	Have compliance audits been conducted to enforce BCP policy and procedures?		
2	Have the systems and resources that will contribute to the mitigation process been identified, including personnel, facilities, technology, and equipment?		
3	Have the systems and resources been monitored to ensure they will be available when needed?		
	PREVENTION **Avoidance, Deterrence, and Detection**		
1	Are employees motivated to be responsible for avoidance and deterrence and detection?		
2	Have facility security programs to support avoidance and deterrence and detection been established?		
3	Have operational policy and procedures to protect the facilities been developed?		
4	Is it ensured that sufficient physical security systems and planning are in place to protect the facility?		
	RESPONSE **Potential Crisis Recognition and Team Notification**		
1	Will the response program recognize when a crisis occurs and provide some level of response?		
2	Have the danger signals been identified that indicate a crisis is imminent?		
3	Has a notification system been put in place, including redundant systems?		
4	Is the notification contact list complete and up to date?		
	RESPONSE **Assess the Situation**		
1	Has an assessment process to address the severity and impact of the crisis been developed?		
2	Has the responsibility for declaring a crisis, with first and second		

	alternates, been assigned?		
	RESPONSE **Declare a Crisis**		
1	Have the criteria been established for when a crisis should be declared?		
2	Has the responsibility for declaring a crisis been clearly defined and assigned?		
3	Has an alert network for BCP Team members and employees been established?		
4	Is it ensured that there is an alternate means of warning if the alert network fails?		
5	Have the activities that will be implemented in event of a crisis been identified, including notification, evacuation, relocation, alternate site activation, team deployment, operational changes, etc?		
	RESPONSE **Execute the Plan**		
1	Has consideration been given to developing the BCP around a ‘‘worst case scenario?’’		
2	Has the BCP been prioritized to save lives, protect assets, restore critical business processes and systems, reduce the length of the interruption, protect reputation, control media coverage, and maintain customer relations?		
3	Have the severity of the crisis and the appropriate response been determined?		
	RESPONSE **Communications**		
1	Has a crisis communications strategy been developed?		
2	Are communications timely, honest, and objective?		
3	Are communications with all employees occurring at approximately the same time?		
4	Are regular updates provided, including notification of when the next update will be issued?		
5	Has a primary spokesperson and back-up spokespersons been designated who will manage and disseminate crisis communications to the media and others?		
	RESPONSE Resource Management – Human Element		
1	Has a system been devised by which all personnel can be accounted for quickly?		
2	Is there a system to ensure current and accurate contact information is maintained?		
3	Have arrangements been made for next-of-kin notifications?		
4	Can crisis counselling be arranged as necessary?		
5	Will the financial systems for payroll and support of facilities and employees remain functional?		
	RESPONSE **Resource Management—Logistics**		
1	Has a designated Crisis Management Center been identified, and does it have necessary life support functions, including uninterruptible power supply and communications equipment?		

2	Have alternate worksites for business resumption and recovery been identified?		
3	Have critical and vital records been stored at an offsite storage facility?		
4	How long can each business function operate effectively without normal data input storage processes?		
5	What must be done to restore data to the same previous point in time within the recovery time objective?		
6	Can any alternate data storage processes be used, after the initial data recovery, to speed the forward recovery to the present time?		
	RESPONSE **Resource Management – Financial Issues and Insurance, Transportation, Suppliers/Service Providers, and Mutual Aid**		
1	Has the appropriate insurance coverage been identified and obtained?		
2	Are cash and credit available to the BCP Team?		
3	Have transportation alternatives been arranged in advance?		
4	Have critical vendor and service provider agreements been established?		
5	Have mutual aid agreements been established?		
6	If so, are they legally sound, properly documented, and understood by all parties?		
	RECOVERY AND RESUMPTION **Damage and Impact Assessment, Process Resumption, and Return to Normal Operations**		
1	Has a damage assessment been performed as soon as possible?		
2	Has the Damage Assessment Team been mobilized to the site?		
3	Has business process recovery been prioritized to recover the most critical business processes first?		
4	Is the schedule of the processes to be restored in accordance with the prioritization schedule?		
5	Is there documentation of when the processes were resumed?		
6	Has the organization returned to normal operations?		
7	Has the decision to return to normal operations been documented and communicated?		
	IMPLEMENTING AND MAINTAINING THE PLAN **Education and Training**		
1	Are the Crisis Management and Response Teams educated about their responsibilities and duties?		
2	Has a checklist of critical actions and responsibilities and duties been developed?		
3	Do Teams receive annual training?		
	IMPLEMENTING AND MAINTAINING THE PLAN **Testing**		
1	Are the Business Continuity Plan and appropriate Teams tested to reveal any weaknesses that require correction?		
2	Have goals and expectations of testing and drills been established?		
3	Are drills and tabletop exercises conducted on an annual basis?		
4	Has responsibility for testing the BCP been assigned with		

	consideration for establishing a test team?		
5	Does test participation include various groups from the organization and the public sector?		
6	Have observers been assigned who will take notes during the test and critique the test at the conclusion of the exercise?		
7	Have tests and drills been evaluated, including assessing how well the goals and objectives of the tests and drills were met?		
	IMPLEMENTING AND MAINTAINING THE PLAN **BCP Review and Maintenance Schedules**		
1	Is the BCP regularly reviewed and evaluated on a pre-determined schedule?		
2	Is the BCP reviewed every time a Risk Assessment is completed for the organization?		
3	Is the BCP modified as needed based on test/exercise results?		
4	Has responsibility for on-going BCP maintenance been assigned?		
5	Does BCP maintenance reflect changes in the operation of the organization?		