

Business Continuity Plan

Insert Name of National Society

[All text in red in this template is provided as reference only and should be removed and / or replaced by National Society specific information.]

Purpose of document:

Business Continuity Planning (BCP) is an essential and ongoing process owned and guided by the National Society's senior management. It ensures that the National Society continues to function during times of crisis and resumes business processes when its programs have been disrupted unexpectedly. The Red Cross Movement plays a critical role in the delivery of regular social and health services (e.g. support to elderly, marginalized groups, people with disabilities, blood donations, etc.), in disaster preparedness and in response. Given this responsibility, disruptions in a National Society's service should be minimised in order to maintain public trust and confidence in its emergency response capabilities.

The purpose of this document is to assist National Societies implement the concepts, practices and processes contained in the IFRC's Business Continuity Planning Guidelines. It provides an array set related information and tools designed to facilitate National Societies who may be at different stages in their efforts initiate, modify or enhance their Business Continuity Plans.

Table of Contents

Part 1: Preparing for Business Continuity Planning:	3
Part 2: Risk analysis:	5
2.1. Scenario development:	5
Step 1: Threat Assessment:	5
Step 2: Vulnerability Assessment:	7
Step 3: Risk Assessment:	8
2.2. Implications for internal systems:	9
Step 4: Business Impact Analysis:	9
Part 3: Business Continuity Preparedness Actions	13
3.1. Financial sustainability:	13
3.2. Staff and volunteer insurance:	14
3.3. Standby Delegations of Financial and Mission Authority:	14
3.4. Offsite Office and Storage Provisions:	14
3.5. Service Providers & Suppliers:	14
3.6. Transportation:	14
3.7. Mutual Aid Agreements:	15
3.8. Security and Safety Standards:	15
3.9. Staff and Volunteer Orientation and Training:	15
3.10. Internal communications / human resource management:	16
Part 4: Response Management:	17
4.1. The Critical Response Management Team	17
4.2. Critical Incident Staff:	18
4.3 Declaration of Level of Alert:	19
4.4 Activating the Critical Response Management Team:	21
4.5 Activation of Business Continuity Measures:	23
4.6 Transition and De-activation:	25
Part 5: Reviewing and updating the BCP:	26
5.1. Revise strategies and plans based on new information and hazard response experience:	26
5.2. Explore future complex crises and implications for the NS:	27
5.3. Learning and adapting – Preparing internal systems for the complex crises of tomorrow:	27
Part 6: Business Continuity Planning Checklist:	28
Part 7: Business Continuity Plan Approval:	32
Annexes:	33
Annex 1: Key contact numbers:	33
Annex 2: Critical function considerations:	35
Annex 3: Terms of Reference example – Critical Response Management Team (CRMT):	37
Annex 4: Terms of Reference example – Operations Response Team (ORT):	39
Annex 5: Emergency Operations Centre functions:	42

Part 1: Preparing for Business Continuity Planning:

For a Business Continuity Planning process to be successful, its contribution to overall NS preparedness efforts must be clear, it must be clearly stated as a priority for leadership and it must receive dedicated financial and human resources.

1.1. Senior Leadership Mandate:

The BCP complements other NS preparedness initiatives and ensures that the organization is always able to fulfil its humanitarian commitments. These commitments and complementary preparedness efforts are outlined in the following National Society documents:

Table 1: Documents outlining the NS Mandate of relevance to BCP

Name of document	Date of publication (or latest update)
<i>Example: Document outlining NS role and mandate in country (Constitution, Red Cross law, Civil Protection mechanism, other government documents where NS role is mentioned, etc.)</i>	
<i>Example: Current NS Contingency plans (specify hazard focus, e.g. typhoon, flood, multi-hazard, pandemic...)</i>	
<i>Example: National Society capacity assessments (OCAC, BOCA, PER, technical assessments)</i>	

1.2. Financial commitment:

Senior management supports not only the planning process but should also ensure the financial resources needed to initiate and maintain the BCP process. This may involve direct funding for the initiative and/or requiring the budget allocations to be contributed by the various National Society units and departments. The following table can be used to scope out the anticipated actions needed, and allied funds anticipated for the BCP effort.

Table 2: Financial resources for BCP

Specific BCP activity	Cost	Source
<i>Example: Meeting of HQ staff members to develop BCP 2 meetings /week x 4 weeks x [cost] =</i>		
<i>Example: Travel of Branch representatives to participate in BCP planning process 10 participants x cost =</i>		
<i>Example: temporary staff / consultants for the development of the BCP</i>		
<i>Example: testing of the plan, training the staff, dissemination of the plan to staff & volunteers</i>		
Total		

1.3. Political and human commitment:

Senior management supports not only the planning process but also the development of the infrastructure and mechanisms necessary to develop implement and maintain Business Continuity Plans. This articulated focus and endorsement ensures that management, staff and volunteers at all levels within the organization understand that BCP is a critical top management priority. Every department / unit and branch / chapter of the National Society should play an active role in the business continuity planning process. Individual roles and responsibilities can be outlined by using the following table.

Table 3: Leadership endorsement and human resources for BCP

Name of department/ unit	BCP endorsed by (name of Department / unit head)	Focal point in department / unit for business continuity planning	Time allocation of focal point (# of hours per week; # of weeks of involvement)	Financial resources allocated to the process
<i>Office of the Secretary General</i>	<i>Jane Doe (SG)</i>	<i>Richard Roe (head of office)</i>	<i>4 hrs. / week x 3 weeks</i>	<i>N/A</i>
<i>Human Resources Department</i>				
<i>Finance Department</i>				
<i>IT Department</i>				
<i>Disaster Department</i>				
<i>Health Department</i>				

1.4. Business Continuity Planning Team:

The Business Continuity Planning Team is tasked with the responsibility developing the BCP. The team includes managers and technical expert staff from all major departments, branch representatives and volunteer groups, nominated by the individual department heads and approved by senior management. The Business Continuity Planning Team Chairperson will be appointed by the NS senior management. The following table is an example outline of a Business Continuity Planning Team.

Table 4: Membership of the Business Continuity Planning Team

Name of department/ unit	Lead name & position	Back-up name & position
<i>Team members and departments represented will vary depending on the individual National Societies. E.g:</i>		
<i>BCP Chairman</i>		
<i>Programs (2-3 Representatives)</i>		
<i>External Communications</i>		
<i>Human Resources & Staff Health</i>		
<i>Finance</i>		
<i>IT / Telecom Unit</i>		
<i>Logistics</i>		
<i>Security</i>		
<i>Organizational Development</i>		
<i>Youth and Volunteer</i>		
<i>Branch Representatives</i>		

If relevant, the National Society may choose to add Terms of Reference for the different positions.

 See Annex 1.2 for key contact numbers.

Part 2: Risk analysis

This section looks at the identification and anticipation of shocks, both internal and external, in current multi-hazard environments. As the National Society adapts to new operational environments, it identifies current risks and their potential impacts, to better identify mitigating measures.

Risk analysis for the purpose of business continuity planning can be approached along five steps:



2.1. Scenario development

If available, the scenario development process should build on existing Contingency Planning processes of the NSs. Based on existing NS/government Contingency planning scenarios, additional risks can be identified.

Step 1: Threat Assessment

The Threat Assessment considers the range of potential hazards within the NS operating environment. This includes natural and human-made hazards, of various scope and magnitude, against a continuum of recurring and non-recurring onsets. The assessment also considers potential hazards with no history along with complex and compound events that may involve the intersection of two or more hazards. For example, the impact of the COVID-19 pandemic on a National Society's service programs and business practices add complexity to pre-existing threats such as recurring flood and typhoon seasons. These hazards will be approached differently in the light of the risks that they pose during a COVID-19 outbreak, considering potential social/physical distancing and quarantine measures that will be in place as well as the economic and social impact for the NS and broader society.

Chart 1: Mapping External Threats

Example of a brainstorming mapping (simplified):¹

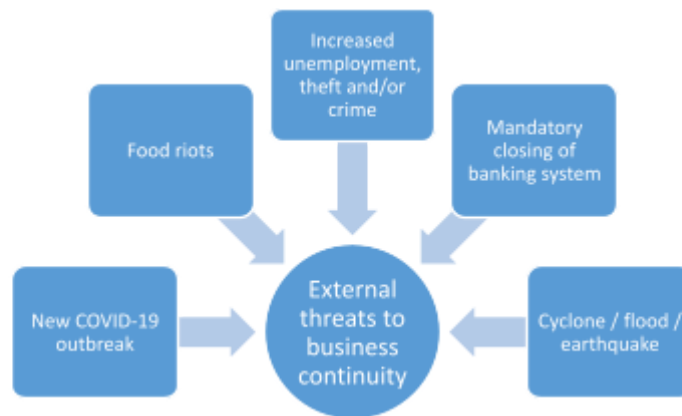


Chart 2: Mapping of internal threats (independently of the external threats)

Example of a brainstorming mapping (simplified):²



¹ Identify 5-7 key external threats for the National Society, considering the COVID-19 pandemic, but also non-COVID related risks. The process should include all BCP department / unit focal points. A collective brainstorming is recommended. Where relevant, the process should be NS scenario planning to existing Contingency Planning efforts and scenarios therein.

- External resources can be helpful to guide the brainstorming sessions, for instance [ACAPS](#).
- For natural threats, historical data concerning frequency of occurrence for given disasters such as tornadoes, hurricanes, floods, fire, or earthquakes helps determine the credibility of the given threat, etc.
- Man-made threats should also be considered, e.g. criminal threats, militant acts, technological hazards, spill of hazardous substances, financial shocks, blackouts, accidents, etc.

² For financial risks, refer to Guidance and Toolkit for NS Financial Sustainability in response to COVID-19 and its economic impact, especially [Tool #2](#).

Step 2: Vulnerability Assessment

Based on the internal and external threats under consideration, the following table provides a list of the factors that make the National Society vulnerable, for both headquarters and branches:³

Table 5: List of NS vulnerabilities and capacities

Threat (see “Threat assessment” above)	NS capability (Consider NS mandate, areas of expertise, financial resources, etc.)	NS Vulnerability at headquarters level (Consider internal systems, financial constraints, impact on staff and volunteers, etc.)	NS vulnerability at branch level (Consider internal systems, financial constraints, impact on staff and volunteers, etc.)
External threats			
<i>Example: Large scale disaster (flood, cyclone, etc.)</i>	<i>Example: Clear mandate and experience in responding to past floods; experienced teams on the ground in risk-prone areas; good relations with donors; etc.</i>	<i>Example: SOPs not in place for remote activation of Emergency Operations Centre; HQ staff not available for field deployment due to restrictions on movements; etc.</i>	<i>Example: systems not in place for remote onboarding of new volunteers; insufficient PPE for new volunteers; etc.</i>
Internal threats			
<i>Example: Funds reallocated by donors from disaster preparedness to COVID-19 response</i>	<i>Example: strong trust from donors; ability to shift other funds to ongoing projects; etc.</i>	<i>Example: Funding for project staff no longer available; NS strategy no longer aligned with key donors; need to retrain resource mobilization department; etc.</i>	<i>Example: current activities no longer aligned with new donor guidelines; gaps in community needs and expectations for NS support; etc.</i>
<i>Example: Fundraising activities cancelled (e.g. first aid courses; small donor outreach; fundraising events)</i>	<i>Example: piloting online donations; new private sector partners interested in supporting NS; etc.</i>	<i>Example: Core HQ positions on hold; recruitments on hold; etc.</i>	<i>Example: volunteer stipends for seasonal preparedness activities on hold; local budgets (for gasoline, electricity, etc.) cut back; etc.</i>

³ The identification of key NS vulnerabilities should involve all units and departments, in turn the vulnerabilities can be assigned to specific NS components significantly impacted by a particular threat, e.g. Finance Department for threats related to access to funds; Volunteer department for threats related to volunteer processes; etc.

During the Vulnerability process, please consider:

- 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, and affected population.

Step 3: Risk Assessment

This step identifies key risks for the National Society based on likelihood and potential onset and impact of the threats. The following chart presents an outline of examined threats from the Threat Assessment in Step 1 in terms of their probability of occurrence and magnitude of impact. In short, while those threats of significant magnitude and probability of occurrence suggests prompt attention, less probable threats with a potential significant impact should not be ignored.⁴

Table 6: Risk table

		Impact Level			
		Minor	Moderate	Severe	Critical
Likelihood	Frequent/ Imminent	E.g. second wave of virus infection		E.g. second wave of COVID-19	
	Probable	E.g. annual floods			E.g. typhoon hitting capital area
	Sporadic			E.g. earthquake in secondary city	
	Low		E.g. sudden decrease in volunteer recruitment	E.g. suspension of banking services	E.g. corruption scandal involving NS leadership

	Catastrophic Situation <i>Undesirable, immediate action required</i>
	Disaster situation <i>Undesirable, priority action - Contingency plans developed and tested.</i>
	Emergency situation <i>Requires heightened awareness and specific procedures.</i>
	Normal situation <i>Managed by routine procedures.</i>

⁴ As with the Vulnerability Assessment, the Risk Assessment should involve all the NS departments and units. Again, the risks can be assigned to specific NS unit or department representative most familiar with or impacted by a threat, e.g. Finance Department for threats related to access to funds; Volunteer department for threats related to volunteer processes; etc.

2.2. Implications for internal systems

Step 4: Business Impact Analysis

The Business Impact Analysis (BIA) seeks to identify, within the various National Society functions, the activities necessary for its survival and ability to fulfil its mission. A key objective of the BCP is to reduce or to mitigate NS risks to an acceptable level for the continuity of the business.

- The term “core function” is used to describe an interrelated cluster of activities organised to support an organization’s operation and the pursuit of its mandate or mission. These functions need to be protected, whether there is an emergency or not; these roles may not directly link to “service delivery” but are essential for the existence of the organisation. Examples include Human Resources, Accounting, External Communications, and Logistics Departments.
- The terms “Critical and Essential Tasks” are in turn used to identify a subset of specific actions or activities within a function that are of high priority and absolutely necessary for the organization to properly operate and achieve its goals. An example includes hiring of response staff by the Human Resources team.

The following table seeks to demonstrate which components of the National Society will likely be most impacted by an incident and what effect it will have upon the organization.

See Annex 2 for Critical functions considerations.

Table 7: Business Impact Analysis

Use this table to complete a Business Impact Analysis. Feel free to add, edit or delete the suggested Departments and assigned Critical Functions as you see fit in your current organizational context.

Function/Department Critical Tasks	Impact of the identified threat (see Step 1)	Maximum time out	Preparedness and Response Action	Responsible Person	Status
Governance & Senior Leadership • General Assembly • National Governing Board • Secretary General • Finance Manager • Branch Governing Board • Branch Secretary	<i>Cannot organize a face to face meeting during the COVID-19</i>	<i>No acceptable time out</i>	<i>Establish IT tools and protocols for remote meetings</i>	<i>Secretary General</i>	
	<i>Overwhelming disaster and service demands put competence and reputation of the NS is into question</i>	<i>No acceptable time out</i>	<i>Senior NS official uses media to accurately describe NS services and related expectations</i>	<i>Secretary General</i>	
Finance and Accounting / Service providers • Cash availability • Funds transfer management. • Payroll continuity. • Accounts payable and receivable	<i>The NS is unable to meet its mission requirements due signing authority requirements (for instance, SOPs that require physical signatures for financial transactions.</i>	<i>No acceptable time out</i>	<i>Periodic back up has been routinely made of all Finance and Accounting Computer files and placed with safe off-site storage</i> <i>Activate alternative mechanisms</i>		

	<i>Staff experience morale and additional personal hardships because of payroll disruptions</i>		<i>Implemented for payroll continuity, Accounts Payable and Receivable, and for regular banking services.</i>		
Human Resources / Consultants • Contracts and payroll management. • Staff and volunteer health education and monitoring • Counselling and psychological support. • Staff movement monitoring and emergency contact list updates. • Staff and volunteer Insurance coverage and claims management.	<i>Insufficient personal protective equipment and training on safety equipment; insufficient safety measures</i> <i>NS unable to meet its mission requirements.</i>	<i>No acceptable time out</i>	<i>Core HR support systems have pre-determined capacity to deal with increased demands, alternative support options have been identified and available for application.</i>		
Disaster Response Management • Deployment of technical experts • Providing of DRM services from assessment to response	<i>Disruption and/or complications in ongoing disaster response and service delivery</i>	<i>No acceptable time out</i>	<i>Support Branches in monitoring and reporting, information management, coordination and activation of response tools</i>		
Health Services • Provision of Relief Health Services • Continuation of ambulance services • operation of medical centres • Medical Equipment & Stock Management • External Medical System Liaison	<i>Service demands potentially overwhelm current systems and available personnel.</i>	<i>No acceptable time out</i>			
Information & Communication Technology, • All automation, telephone and mobile communication systems are operational. • Telecommuting for essential staff to work from home (equipment provided, online access to files assured) • Help line support is maintained. • Alternative power supply and surge protection is readily available	<i>Automation, telephone and mobile communication systems interruption or failure will either inhibit or prevent the NS from meeting its mission requirements.</i>	<i>No acceptable time out</i>	<i>A Disaster Recovery Automation and Telecommunication Plan has been developed and is activated.</i> <i>Pre-incident fail safe and backup systems are in place and activated backup systems are activated'</i> <i>Incident Backup schedule is implemented.</i> <i>Computer files are routinely copied and placed with safe off- site storage.</i>		

• Phone service continuity and back up communications in case of service interruption.					
Volunteer Management • Spontaneous volunteers are quickly screened, oriented and assigned. • Volunteers are appropriately supervised. • Volunteers are appropriately recognised.	<i>Massive Influx of volunteers overwhelms training system and supervision capacity. New volunteers unable to secure insurance coverage appropriate for the incident. The NS is faced with liability issues diverting attention and resources from its mission.</i>	<i>1 to 3 days</i>	<i>Volunteer support systems have designed excess capacity to accommodate sudden influx of volunteers. Training support has expansion flexibility for increased supervisor training. Insurance coverage negotiated prior to event and in place to accommodate new volunteers.</i>		
Security management. • Staff and volunteer safety. • Building and physical asset security	<i>Buildings along with physical assets are at risk due to potential contamination. Vehicles impacted by limited availability of fuel.</i>	<i>No acceptable time out</i>	<i>Staff and volunteer guidance developed pre-incident and readily available for distribution; building security SOP's are implemented along with alternative fuel access arrangements, security of external / third party service providers (e.g. catering services, consultants)</i>		
Logistics and Procurement. • Inventory of services and equipment to be accessed during an emergency. • Procurement and stock management • Shipping and handling	<i>Standard suppliers cannot deliver services, products and equipment necessary for the NS mission</i>	<i>No acceptable time out</i>	<i>Backup contracts and secondary suppliers, arranged for pre-incident, and are activated.</i> <i>Stockpiling of pre-identified items / equipment, medical logistics</i>		
Internet and Web- Site Management. • Publishing, editing and maintenance • ...	<i>Valuable information about the incident and the NS response cannot be provided to beneficiaries and the general public</i>	<i>No acceptable time-out</i>	<i>Internet and Web-Site Disaster Recovery Plan is implemented.</i>		
Facilities Management. • Facilities are operational; • Suitable alternative sites available if needed.	<i>Staff and volunteers' effectiveness hindered by unsuitable working environment.</i>	<i>1 to 2 days</i>	<i>Cleaning and Hygiene along with backup maintenance arrangements are in place and activated along with heat, air conditioning and ventilation support alternatives.</i>		

External Information and Communication	<i>Communication link disruption; compounded by a significant increase in media attention</i>	<i>No acceptable time-out</i>	<i>External media contacts are maintained and augmented as needed thru implementation of the NS Automation and Communications Disaster Recovery SOPs.</i>		
Office Equipment and Supplies Management	<i>Mission needed supplies and equipment are not available when needed</i>	<i>No acceptable time out</i>	<i>Working facilities are cleaned and sanitised daily; office supply inventories are maintained</i>		
Vital Records Management.	<i>Financial and legal liabilities arise during the NS response causing the diversion of attention and resources</i>	<i>No acceptable time out</i>	<i>Vital records are safely stored and automated files backed up via pre-incident contracts and arrangements</i>		

Part 3: Business Continuity Preparedness Actions

The Risk Management Plan is a concise document, sanctioned by the National Society's senior leadership, detailing the Risk Management process and actions to be taken by the National Society. It is based on the information and findings of the Risk Analysis, the Vulnerability Assessment and Business Impact Analysis. Each corresponding department will define roles, responsibilities, the resource commitment, and realistic timelines for the goals, objectives, benchmarks, and performance expectations that the strategy is designed to achieve. The Plan will be shared with National Society staff and volunteers. It will be routinely updated and may be changed or enhanced over time to accommodate new and evolving internal and external conditions.

2.1. Financial sustainability

The NS determines the core cost to exist and run its mandate as defined by key governing articles (e.g. statutes, constitution and auxiliary role to government) – the minimum cost for a national society to exist and fulfil its mandate (guided by its legal base and statutory obligations). As part of business continuity, the NS must consider how to sustain the resources to cover the costs that are defined as “core” to the organisation.

Core Cost	Detail
Legal/constitutional or statutory costs	• <i>IFRC Statutory Contribution</i> • <i>Attendance at Movement statutory meetings-</i>
Governance costs	• <i>Board meeting or AGM expenses</i> • <i>Board member allowances (including travel cost if necessary)</i>
General administration	• <i>Printing and stationery</i> • <i>Annual audit fees</i>
Salary and costs for the core structure	• <i>Salaries for staff listed in core structure</i> • <i>Additional legislative costs for staff listed in core structure</i>
Volunteer costs for core services	• <i>Volunteer allowances</i> • <i>Volunteer insurance</i>
Headquarter and branch utilities, IT and communications costs	• <i>Electricity and water</i> • <i>Telephone and internet connectivity (including video conferencing equipment)</i> • <i>Postage and couriers</i>
Maintenance for core assets	• <i>Upkeep of headquarters and branch offices</i> • <i>Maintenance of non-program vehicles</i>
Essential running costs	• <i>Travel costs for staff and volunteer to implement service</i>

The operational funds (whether “Program Cost/ Project Cost/ Direct Cost” or “Program Support Cost / Indirect Cost / Admin costs”) should not replace the existing practice on how the NS is covering its core cost, as this will undermine the existing capacity of generating funds for the core cost.

2.2. Staff and volunteer insurance

National Societies, within their responsibility for duty of care for their staff and volunteers, have established insurance mechanism covering accidents, illness and compensation in case of death to their families while they are on duty. This is particularly important consideration in the case of high-risk hazards such as pandemics where staff and volunteers may become injured or infected and thus unable to work. In such cases a balance needs to be struck between the mission requirements of the NS and the safety of its staff and volunteers, for the wellbeing of staff and volunteers and because unnecessary exposure of staff and volunteers can damage the reputation of the organization

[Insert detail on NS staff and volunteer insurance measures.]

2.3. Standby Delegations of Financial and Mission Authority

In the event of a disruption of the NS standing line of financial and administrative authority, alternative officials will step in to fill the void, within clear definitions of circumstances, scope of authority and limits. This will ensure that the NS can make critical decisions and commitments in a timely manner and ensure accountability.

[Insert detail on standby delegations of financial and mission authority. Any specific Emergency Procedure for finance, HR, volunteering, logistics, IT etc. should be mentioned here or included as an annex.]

2.4. Offsite Office and Storage Provisions

Depending on the nature and scope of the hazards under consideration, the BCP details provisions for staff to work from home or go to alternate facilities. Both situations need to include appropriate communication and automation support.

[Insert detail on offsite office and include if needed additional or alternative sites for the storage and maintenance of mission critical supplies, equipment and vehicles.]

2.5. Service Providers & Suppliers

The stockpiling of "mission-critical" supplies (those without which the business cannot function) is essential to mitigate the impact on the NS in the event suppliers (or the marketplace) cannot continue to provide the quantities needed during the emergency.

[Insert detail of framework agreements with vendors for provision of commonly used additional items ahead of the emergency.]

2.6. Transportation

Where possible, goods will be prepositioned across the country to anticipate any potential disruption in transport. Signing framework agreements ahead of time with haulage firms at state / province, regional and national levels will also mitigate such disruptions, to ensure goods can be transported throughout the country during a crisis. Areas where transportation is critical include, but are not limited to:

- Evacuation of personnel
- 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.

[Insert detail of framework agreements with transportation and / or haulage firms. Alternatives should also be considered as during a crisis the normal rule of access may not apply and transportation may be impaired.]

2.7. 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. Special attention should be given to agreement with Government authorities especially related to the auxiliary role of the NS.

[Insert detail of mutual aid agreements.]

2.8. Security and Safety Standards:

The establishment of security and safety protocols will be indicated based on the hazards under consideration, depending on the operational context. For the current COVID 19, scenarios will continue to be developed based on the number of people infected and how this will affect the operationalization of services and programs in the field and at headquarter level. As some hazards such as pandemics are fast-moving contexts, safety standards may be revised accordingly with little or no warning.

[Insert detail of security and safety standards. For more information concerning the Federation's Critical Incident Management Protocol go to [FedNet](#).]

2.9. Staff and Volunteer Orientation and Training

The Business Continuity Plan must be understood by all staff members and volunteers. Each Business Continuity Planning Team member is responsible for updating the contact lists for their respective teams, including staff and volunteers in branches – collectively, these lists must cover all NS personnel. Individual focal points from each department / unit are tasked with the dissemination of the present plan:

Table 10: NS BCP dissemination strategy

Name of department/ unit	Focal point for business continuity plan dissemination	Mechanism for dissemination	Latest BCP simulation (scheduled and/or surprise)	Financial resources allocated to the process
<i>Office of the Secretary General</i>	<i>Richard Roe (head of office)</i>	<i>2 information sessions as part of weekly staff meetings: 10 June & 17 June</i>	<i>25 June – desktop exercise with all unit staff</i>	<i>N/A</i>
<i>Human Resources Department</i>				
<i>Finance Department</i>				

2.10. Internal communications / human 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. The following must be considered in the Preparedness actions:

- All personnel must be accounted for quickly after the onset of a crisis. The National Society must establish a telephone tree. The phone tree should be tested monthly to ensure contact lists are up to date and that everyone can be contacted, and their location can be known.
 - Maintaining staff contact database up to date is responsibility of: [name of individual; department / unit; and contact information]
 - Maintaining volunteer contact database up to date is responsibility of: [name of individual; department / unit; and contact information]
- All staff and volunteers must know who to contact in any emergency and how to relay any message pertaining to a security incident.
- All personnel must know their roles and tasks in an emergency and be aware of the security implications on their everyday lives.
- Individuals with skill sets should be identified early on, particularly those that can be used during an emergency – these can be both soft (leadership) and hard (technical) skills.
- All staff and volunteers should ensure that the HR Department has the most up-to-date version of their next of kin contacts.
 - Informing staff next-of-kin is responsibility of: [name of individual; department / unit; and contact information]
 - Informing volunteer next-of-kin is responsibility of: [name of individual; department / unit; and contact information]
- Secure essential and sensitive documentation
- Staff to put in place a Family Safety Plan (see IFRC PAPE resource [here](#) – page 33)
- Staff to maintain 2 weeks contingency supplies of personal prescription medicine, and non-prescription medicine
- Identify health facilities in case admissions are necessary.

Part 4: Response Management

4.1. The Critical Response Management Team

Whenever a threatening or occurring event is deemed significant and thus prompting the National Society to prudently implement Business Continuity measures, the Critical Response Management Team, and Critical Incident Staff are activated.

The Critical Response Management Team (CRMT) is a working group predesignated by the NS leadership and composed of representative key NS functions such as Senior Management, Disaster Services, Human Resources, Logistics, Health Services, Volunteers, Information Technology, Security, Legal, Media Relations and other critical support functions. CRMT members are appointed in consultation with and based upon the recommendations of the individual NS departments heads. The CRMT is a decision-making body tasked with guiding the NS through the course of the threatening or occurring incident. The CRMT mission is to keep the NS functioning during the crisis while also overseeing the National Society's external respond to the threat or event. When required by circumstances and conditions, the CRMT will also activate an Operations Response Team.

All CRMT members will have an assigned back-up in the case the CRMT member becomes incapacitated for any reason or cannot be reached in a timely manner. Other NS staff members and volunteers may be seconded to the CRMT to assist its members in planning and execution tasks.

- ❑ See Annex 3 for an example of Terms of Reference for the CRMT.
- ❑ See Annex 4 for an example of Terms of Reference for the Operations Response Team.

Table 8: Critical Response Management Team (CRMT) members

Department represented	Critical staff names & positions	Back-up names & positions
<i>add, edit or delete the suggested Critical Functions / Essential services as you see fit in the current organizational context.</i>	<i>Depending on the number and nature of the Critical Tasks involved, more than one individual can be identified within a function</i>	
<i>SG's Office:</i>		
<i>Finance and Accounting:</i>		
<i>Human Resources:</i>		
<i>Disaster Response Management:</i>		
<i>Health Service:</i>		
<i>Information & Communication Technology:</i>		
<i>Volunteer Management:</i>		
<i>Security Management:</i>		
<i>Logistics & Procurement:</i>		
<i>Internet & Web-Site Management:</i>		
<i>External Information & Communication</i>		
<i>Office Equipment & Supply Management</i>		
<i>Vital Records Management:</i>		

- ❑ See Annex 1.3 for contact information.

4.2. Critical Incident Staff

Critical Incident Staff (CIS) are those *individuals identified as being responsible for carrying out essential tasks* identified within a National Society organizational functions. Each CIS is expected to work throughout the response.

A CIS will be expected to come to the office, but it may become necessary to work from home (for instance due to transportation system disruptions or for health reasons during pandemic outbreaks). Critical Incident Staff include the person responsible for the payment of salaries, the person responsible for ensuring the NS shared drives are always accessible, the execution of financial commitments and other key NS actions.

Back-up critical incident staff (BCIS) are designated individuals appointed to replace a CIS member should that member become incapacitated or otherwise unavailable. The BCIS are to be appointed by their department leader. They are to maintain a close relationship with their CIS counterpart to maintain a detailed working knowledge of their files and issues, and to promptly replace the CIS when needed. Should a BCIS become incapacitated or otherwise unavailable, they must immediately inform their supervisor or manager.

Table 9: Critical Incident Staff

Department represented	CIS Name & Position	Back-up name & position
NS leadership / CMT Lead		
Program teams (2-3 representatives)		
Communications unit		
Human Resources & staff health		
Admin Unit		
Finance Unit		
IT / Telecom Unit		
Logistics Unit		
Security Unit		
Organizational Development Unit		
Volunteerism / Youth unit		

4.3. Declaration of Level of Alert

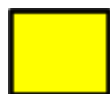
If the NS has a different Alert Phase determination, or if there is an existing Civil Protection emergency alert phase designation in the country, it should be inserted here in place of the text below. This should also include scale up or scale down based on contingency planning definition of crises and recommendations for public organizations (and RC as auxiliary organization might be affected with it).



Green: Normal situation

Triggers:

Default situation, with no major security/health concerns.



Yellow: Emergency situation

External triggers:

General	COVID-19
☐ Government declares state of emergency in some parts of the country ☐ Government closes schools or other public services. ☐ Civil fear, political and social disruption of normal life. ☐ Some closures of schools / key businesses ☐ Some security/health concerns. ☐ Heightened security awareness initiated. ☐ Increase in social unrest and xenophobic or fear-based attacks/behaviours.	☐ Localised transmission has been confirmed ☐ Government issues warnings and advisories to the population (e.g. protective measures like face masks, physical distancing) ☐ Government has indicated that it is considering movement controls and curfews ☐ Country has imported cases that are detected and isolated, resulting in no or limited onward transmission ☐ Quarantine or cordon sanitaire of affected neighbourhoods or broader movement restrictions ☐ Passenger and goods vehicle services at times disrupted due to health scare. ☐ Active health checks at airports, border crossings and ports or borders may be closed

Internal triggers:

General	COVID-19
☐ Working conditions allow programs to continue without significant adaptation: there are some security/ health concerns – a situation of heightened security / health awareness is initiated.	☐ COVID-19 diagnosed among close contacts, colleagues, care providers, etc. ☐ Working conditions allow programs to continue without significant adaptation: there are some security/ health concerns – a situation of heightened security / health awareness is initiated.



Orange: Disaster situation

External triggers:

General	COVID-19
☐ Government declares state of emergency. ☐ Civil fear, political and social disruption of normal life. ☐ Increase in social unrest and xenophobic or fear-based attacks/behaviours. ☐ Tight security management needed ☐ Several injuries or deaths ☐ Closure of main businesses and potentially curfew imposed by government ☐ Moderate community impact.	☐ Community-level transmission occurring across broader population of unrelated people. Response activities shift from containment (e.g. screening, contact tracing) to mitigation (e.g. treatment, essential services support, mitigation of social and economic disruption) ☐ Quarantine or cordon sanitaire of affected regions and/or broader movement restrictions ☐ Health system capacity challenges - e.g. inability to meet demand for intensive care ☐ Government closes schools or other public services and / or prevents mass gatherings or public events. ☐ Government puts in place health related measures like physical distancing, wearing of Face masks in defined areas, further health advice / communication.

	☐ Passenger and goods vehicle services at times disrupted due to health scare. ☐ Active health checks at airports, ☐ Border crossings and ports or borders closed.
--	---

Internal triggers:

General	COVID-19
	☐ Personal protective measures obligatory for RC services. ☐ Epidemic Mitigation Operations, adapt all programming to reduce exposure and/or increase protection – tight health, safety and security management needed ☐ International support mechanism limited / reduced



Red: Catastrophic situation

External triggers:

General	COVID-19
☐ Government declares a national emergency. ☐ Civil power unable to enforce containments measures - martial law is declared ☐ Increased crime and unrest lead the government to deploy the military in an internal security role. ☐ Civil fear, political and social disruption of normal life. ☐ Increase in social unrest and xenophobic or fear-based attacks/behaviours. ☐	☐ Epidemic spreads rapidly and is reported to be overwhelming containment measures ☐ Health services have difficulty coping ☐ Localised transmission has been established and is rapidly increasing ☐ Government closes schools and non-essential public services ☐ Majority of shops, markets and workplaces are closed ☐ Civilian transport considerably reduced due to health and safety concerns.

Internal triggers:

General	COVID-19
	☐ Government has imposed movement restrictions or other measure that impact business continuity ☐ Number of sick staff members is impacting business continuity

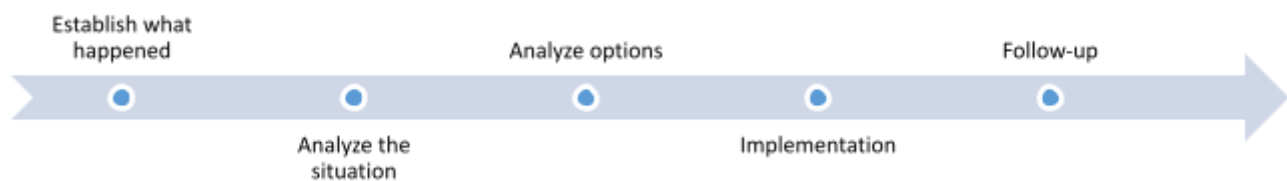
Given current triggers, the National Society is in [Green / Yellow / Orange / Red] Phase.

4.4 Activating the Critical Response Management Team

Once a change of situation has occurred – i.e. once threshold triggers have been reached and generate a change of phase – the Critical Response Management Team is responsible for managing the response to the situation and is relieved from the routine responsibilities of their regular position for the duration of the response. When the CRMT takes over, the lines of authority are simplified to allow immediate, urgent decisions to be made – within the limits around potential liability of the organization. Decisions will be communicated to the Executive Committee / Governing Board and other members of senior management, prior to dissemination to the rest of the organization.

Analysis of the situation

As this process is worked through, it is important to gather as much relevant information as quickly as possible. Regardless of the level of critical incident, the Critical Response Management Team will follow these steps:



External communications

External communications are key in any crisis and needs to be provided accurately and frequently (without leading to communications fatigue). One main role will be to validate information and dispel rumours.

External communications (and the development of the crisis communications strategy) will be coordinated by:

- Primary spokesperson: [name of individual; department / unit; and contact information]
- Proxy: [name of individual; department / unit; and contact information]

Specific 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, for instance:

- Affected Populations and surrounding communities
- Contractors
- Media
- Government, Donor Agencies and Regulatory Agencies
- Local law enforcement
- Emergency responders

The following principles should be followed in the crisis communications strategy:

- Communications should be timely and honest.
- Communications should provide objective and subjective assessments.
- Provide opportunities 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.

- Develop and update key messages and share with all relevant member of the organisation (board, CRMT)

Internal communications / human 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. The following must be considered in the Response Management:

- All personnel must be accounted for quickly after the onset of a crisis. The National Society should use its phone tree to ensure all staff and volunteers are fine.
- Bad news should be given all at once. All employees should be informed at approximately the same time.

In the event of illness or fatalities, arrangements should be made for notification of any next-of-kin, preferably in person by a member of senior management. **See Annex 1.5. for NS Staff phone tree information.**

Emergency Operations Centre (EOC)

Please Note: If the NS maintains an Emergency Operations Centre, then include function and responsibilities of EOC and clarify its relationship to the CRMT

The NS Emergency Operations Centre is located [complete with corresponding information, including any description of facilities. Where possible a secondary EOC should also be identified if the primary centre is impacted by the crisis event.]

In the case of pandemics, it will be recommended that as much as possible work is done remotely with people calling in to minimise the risk of infection.

See Annex 5 for detail of EOC functions.

4.5 Activation of Business Continuity Measures

Declaring a crisis will trigger various contingency actions included, but are not limited to:

- Additional call notifications
- Evacuation, shelter in place, or relocation
- Safety protocols
- Response site and alternate site activation
- Personnel assignments and accessibility
- Emergency contact activation
- Operational changes including the activation of any special Standard Operating Procedures

All incidents need to be reported immediately and where possible a short report developed that details out what happened; location; who was affected and likely implications/follow up.

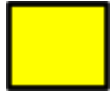


Green: Normal situation

Generic Business Continuity measures:

No adverse threatening or occurring situations are occurring. Routine business practices are conducted; NS focus on planning, preparedness and training activities. In certain situations, there may be steps that

can and should be implemented even without a phase change. Preventative measures may include a reduction in staff physically in the office or for most meetings to be held on-line rather than in person.



Yellow: Emergency situation

Generic Business Continuity measures:

Readiness actions, getting all elements of the BCP ready to be actioned:

- BCP and contingency plans reviewed and confirmed by all departments
- Review logistical agreements / shipments in the pipeline and potentially stockpile relevant equipment
- Activate FbA measures / protocols

COVID-19 Business Continuity measures:

- Prepare to adapt all community-level programming to institute social distancing approaches (1m distance) and reduce or eliminate exposure to respiratory droplets or direct contact with ill people
- Identify high-risk activities which cannot be modified to reduce personnel exposure to contact with/droplets from people with respiratory illness, and plan mitigation measures, including PPE.
- Any staff with mild respiratory symptoms (e.g. runny nose, mild cough) or fever to work from home until symptoms are resolved.
- Establish / promote staff health hotline to support staff with COVID-19 symptoms and provide psychosocial support if feasible
- Personal protective measures prepared as a backup or on a voluntary basis



Orange: Disaster situation

Generic Business Continuity measures:

- Activating parts or all of the Business Continuity Plan
- Any incident is to be reported to xxxxxxxx as soon as possible for further follow up.
- All personnel carry mobile phones (or other emergency communication devices) and essential phone numbers along with them at all times.
- Staff to maintain cash supply and 6 weeks contingency supplies of personal prescription medicine, and non-prescription medicine.

COVID-19 Business Continuity measures:

- No travel to affected communities/ facilities without pre-planning and operational/ humanitarian necessity
- Strict access and movement procedures in office (e.g. temperature screening and handwashing points at entry)
- Any staff with mild respiratory symptoms (e.g. runny nose, mild cough) or fever to work from home until symptoms are resolved.
- Implement programmatic adaptations to reduce or eliminate exposure to respiratory droplets or direct contact with ill people. Ensure any personnel involved in unavoidable contact or clinical service provision has PPE appropriate to the level of exposure, and training to use it.
- Implement mitigation measures, including PPE, for high-risk activities which cannot be modified to reduce personnel exposure to contact with/droplets from people with respiratory illness.



Red: Catastrophic situation

Conditions do not allow work, risk to Red Cross Red Crescent personnel extreme.

Generic Business Continuity measures:

- Major Impact on Business Continuity – Activating parts or all of the Extreme Event Contingency Plan

COVID-19 Business Continuity measures:

- Pandemic or local epidemic exceeds mitigation capacity.
- Hibernation involves remaining in-doors in prepared locations and waiting to see if the situation stabilises. In case of Hibernation staff will be directed to isolate themselves in their homes or office compound. No visitations.
- Any personnel who become seriously ill transferred to identified appropriate local health facility.
- Personnel to ensure that they have communications with supervisor to await further instructions.

4.6 Transition and De-activation

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 subtle changes, particularly in complex situations such as a pandemic. There is a possibility that some measures will be eased for some time but due to a worsening of the situation the alert levels and related measures / restrictions might be tightened again. The Response Management Team will continue to assess the situation carefully to determine what the organization may be able to get back to business. It will review the alert levels and scale down the alert status when supported by events and accomplishments. During this process the Team will also inform staff on subsequent decisions and changing alert status.

Once the crisis has been deemed over by the appropriate governmental authority, the NS will seek to return to the degree possible to a state of 'business as usual', or pre-incident status. Some planning specifically related to follow up communication may likely be required to donors and the general public. The organization will 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.

Part 5: Reviewing and updating the BCP

4.1. Revise strategies and plans based on new information and hazard response experience

The internal and external environment of a National Society is constantly in motion. Periodic changes in leadership, priorities and focus produce changes in a NS structure, resource allocation and service programs. Hazards in the external environment change over time in terms of frequency, scope, and magnitude. Government policy regarding hazards and response evolve. New hazards need to be identified and anticipated, particularly with respect to the unintended consequences of technology, such as the increasing threat of epidemics and pandemics raised in part by global trade and transportation systems. Moreover, the art and science of hazard assessment and emergency management are evolving, with enhanced new information, academic research, professional practice concepts and the lessons learned from occurring catastrophic and disaster events. These different elements must be factored in the National Society's disaster planning, to continuously refine its business continuity planning.

Once the peak of an occurring disaster or crisis has subsided, the National Society should implement a formal debriefing process to learn from the experience, as it applied to both service delivery and business continuity planning. The purpose is to formulate and implement improvements for ongoing BCP and service delivery response actions. Key actions may include:

- ***Exploring and documenting lessons learned***, through the engagement of staff and volunteers. Unpack how the incident was responded to from the start of the process to the end and examine both the actions that took place at every stage, as well as how quickly these were implemented. The process should also analyse the roles different people played and any gaps or challenges that occurred. Gather feedback from workers to improve your plans. Identify any gaps and any needs you may have for additional resources in the future. Lessons learned will be documented and shared with the wider NS team as part of a transparent sharing process. Any specific learnings will be followed up during the 'white' phase to ensure that mechanism is in place prior to any future events. Once these improvements have been made, staff will be invited to attend further trainings to disseminate the findings and recommendations more widely. A simple After- Action Review process could be outlined.
- ***Maintaining and expanding the NS Business Continuity Planning team.***
- ***Revisiting the NS risk assessment and risk management processes.*** Determine ways to improve both the planning and implementation processes. Assess the availability of medical, mental health, and social services for workers.
- ***Updating and testing the National Society's emergency operations and communication plans*** every 12–18 months, particularly as aspects of the NS workplace change. Update the BCP based on lessons learned,
- ***Replacing necessary supplies and equipment***, and based on experience, add new items to the inventory.

4.2. Explore future complex crises and implications for the NS

Futures and Foresight (FF) work plays an increasingly important role in the planning and work of large humanitarian and development organisations to help predict and understand trends that will impact Red Cross Red Crescent work into the future. FF analysis is a way to help think about the long-term issues and challenges associated with achieving a particular objective, or to understand what a future operating environment may look like, and how we may need to respond. FF work helps focus on long (20 years plus) or on short (within the next 5 years) timelines and is primarily used to influence and inform organisational strategy, policy, prioritisation and focus. It can complement conventional forms of analysis and shape short to medium term policy and strategy in a way that is consistent with addressing major long-term challenges. Based on these longer-term scenarios, business continuity plans can be adjusted to reflect previously unanticipated scenarios.

4.3. Learning and adapting – Preparing internal systems for the complex crises of tomorrow

Regular maintenance of the BCP cannot be overemphasised. 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.*

In order to remain relevant to a constantly evolving environment, the BCP needs to be constantly updated, and that the changes are promptly shared with all relevant National Society departments and Officials. It is the responsibility of [indicate name of individual and corresponding department / unit] to update the Business Continuity Plan. This includes the daily collection of information to monitor the changing situation.

- The updating of the plan should be completed at the latest by [indicate deadline – ideally every week initially].
- This information will be used to determine whether specific triggers have been reached and whether the assessment of Phase determination should be changed.
- Training will be provided to all relevant staff and volunteers. They will be briefed on the key components of the BCP, as well as the Response Plans that affect them directly. Such training will also 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.
- The BCP will also be reviewed every time a risk assessment is completed for the organization. The results of the risk assessment will help determine whether the BCP continues to adequately address the risks facing the organization.
- Based on exercise results (simulation; tabletop), the BCP should be modified as necessary.

The BCP will be updated by: _____

The process to update the plan will take place: _____

Part 6: Business Continuity Planning Checklist

	Business Continuity Guideline Checklist	Y/N	Document reference
	Considerations		
1	If a major disaster occurred today, has your organization planned for survival?		General
2	Does your organization have a Business Continuity Plan (BCP), and is it up to date?		General
3	Has senior management approved the BCP?		General
4	Does senior management support the BCP?		Part 1 & 7
5	Has the cost of the BCP been determined, including development and maintenance?		Part 1
6	Have the initial audit, security, and insurance departments reviewed the BCP?		Part 7
7	Has the BCP been tested, including a surprise test?		Part 3
	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?		Part 1
3	Has a BCP Team been appointed, and does it include senior business function leaders?		Part 1
4	Has the BCP been communicated throughout the organization?		Part 3
5	Has a person been assigned with the responsibility to update the BCP?		Part 5
	DEVELOPING THE PLAN		
	Risk Assessment		
1	Has your organization conducted a multi-hazard Risk Assessment?		Part 2
2	Have the types of risks that may impact your organization been identified and analysed?		Part 2
3	Has the likelihood for each type of risk been rated?		Part 2
	DEVELOPING THE PLAN		
	Business Impact Analysis		
1	Have the critical business processes been identified?		Part 2
2	If a crisis were to happen, has the impact, in terms of human and financial costs, been assessed?		Part 2
3	Have the maximum allowable outage and recovery time objectives been determined?		Part 2
4	Has the length of time your organization's business processes could be non-functional been determined?		Part 2
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?		Part 3
2	Have plans and procedures to respond to any incident been developed?		Part 4
3	Have strategies that address short- and long-term business interruptions been selected?		Part 3
4	Are the strategies attainable, tested and cost effective?		Part 3
	DEVELOPING THE PLAN		
	Crisis Management and Response Team Development		
1	Is the Crisis Management Team comprised of members from human resources?		Part 2

2	Have response plans to address the various aspects of the crisis been developed and incorporated into the organization's overall BCP?		Part 4
3	Do the response plans address damage assessment, site restoration, payroll, human resources, information technology and administrative support?		Part 4
4	Has contact information been included in the plan for the Crisis Management and the Response Teams?		Part 2
PREVENTION Compliance w/Corporate Policy & Mitigation Strategies			
1	Have compliance audits been conducted to enforce BCP policy and procedures?		Part 2
2	Have the systems and resources that will contribute to the mitigation process been identified, including personnel, facilities, technology and equipment?		Part 3
3	Have the systems and resources been monitored to ensure they will be available when needed?		Part 3
PREVENTION Avoidance, Deterrence, and Detection			
1	Are employees motivated to be responsible for avoidance, deterrence and detection?		-
2	Have facility security programs to support avoidance and deterrence, 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 recognise when a crisis occurs and provide some level of response?		Part 4
2	Have the danger signals been identified that indicate a crisis is imminent?		Part 4
3	Has a notification system been put in place, including redundant systems?		Part 4
4	Is the notification contact list complete and up to date?		Annex 1
RESPONSE Assess the Situation			
1	Has an assessment process to address the severity and impact of the crisis been developed?		Part 4
2	Has the responsibility for declaring a crisis, with first and second alternates, been assigned?		Part 4
RESPONSE Declare a Crisis			
1	Have the criteria been established for when a crisis should be declared?		Part 4
2	Has the responsibility for declaring a crisis been clearly defined and assigned?		Part 4
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.?		Part 4
RESPONSE Execute the Plan			
1	Has consideration been given to developing the BCP around a "worst case scenario?"		-
2	Has the BCP been prioritised 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?		Part 3
3	Have the severity of the crisis and the appropriate response been determined?		Part 4

	RESPONSE Communications		
1	Has a crisis communications strategy been developed?		Part 4
2	Are communications timely, honest and objective?		Part 4
3	Are communications with all employees occurring at approximately the same time?		Part 4
4	Are regular updates provided, including notification of when the next update will be issued?		Part 4
5	Has a primary spokesperson and back-up spokespersons been designated who will manage and disseminate crisis communications to the media and others?		Part 4
	RESPONSE Resource Management – Human Element		
1	Has a system been devised by which all personnel can be accounted for quickly?		Part 4
2	Is there a system to ensure current and accurate contact information is maintained?		Part 4
3	Have arrangements been made for next-of-kin notifications?		Part 4
4	Can crisis counselling be arranged as necessary?		-
5	Will the financial systems for payroll and support of facilities and employees remain functional?		Part 4
	RESPONSE Resource Management—Logistics		
1	Has a designated Crisis Management Centre been identified, and does it have necessary life support functions, including uninterruptible power supply and communications equipment?		Part 2
2	Have alternate worksites for business resumption and recovery been identified?		Part 2
3	Have critical and vital records been stored at an offsite storage facility?		Part 2
4	How long can each business function operate effectively without normal data input storage processes?		Part 2
5	What must be done to restore data to the same previous point in time within the recovery time objective?		Part 2
6	Can any alternate data storage processes be used, after the initial data recovery, to speed the forward recovery to the present time?		Part 2
	RESPONSE Resource Management – Financial Issues and Insurance, Transportation, Suppliers/Service Providers, and Mutual Aid		
1	Has the appropriate insurance coverage been identified and obtained?		Part 3
2	Are cash and credit available to the BCP Team?		Part 3
3	Have transportation alternatives been arranged in advance?		Part 3
4	Have critical vendor and service provider agreements been established?		Part 3
5	Have mutual aid agreements been established?		Part 3
6	If so, are they legally sound, properly documented, and understood by all parties?		Part 3
	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?		Part 4
2	Has the Damage Assessment Team been mobilised to the site?		-
3	Has business process recovery been prioritised to recover the most critical business processes first?		Part 4
4	Is the schedule of the processes to be restored in accordance with the prioritization schedule?		Part 4
5	Is there documentation of when the processes were resumed?		-
6	Has the organization returned to normal operations?		Part 4

7	Has the decision to return to normal operations been documented and communicated?		Part 4
IMPLEMENTING AND MAINTAINING THE PLAN Education and Training			
1	Are the Crisis Management and Response Teams educated about their responsibilities and duties?		Part 4
2	Has a checklist of critical actions and responsibilities and duties been developed?		Part 4
3	Do Teams receive annual training?		Part 3
IMPLEMENTING AND MAINTAINING THE PLAN Testing			
1	Are the Business Continuity Plan and appropriate Teams tested to reveal any weaknesses that require correction?		Part 3
2	Have goals and expectations of testing and drills been established?		Part 3
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?		Part 3
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?		Part 5
2	Is the BCP reviewed every time a Risk Assessment is completed for the organization?		Part 5
3	Is the BCP modified as needed based on test/exercise results?		Part 5
4	Has responsibility for on-going BCP maintenance been assigned?		Part 5
5	Does BCP maintenance reflect changes in the operation of the organization?		Part 5

Part 7: Business Continuity Plan Approval

Department represented	Name & title	Signature	Date endorsed
NS Secretary General			
Audit Unit			
Insurance Unit			
Security Unit			
Programs Unit			
Communications Unit			
Human Resources & staff health			
Admin Unit			
Finance Unit			
IT / Telecom Unit			
Logistics Unit			
Security Unit			
Organizational Development Unit			
Volunteerism / Youth unit			

Annexes

Annex 1: Key contact numbers

Annex 1.1: Key contact numbers – COVID response

Service	Phone number / Contact info
National Society Health Hotline	
IT Support for remote workers (work from home)	
COVID-19 Hotline	

Annex 1.2: Key contact numbers – Business Continuity Planning Team

Department represented	Lead name & position	Lead contact (office & cell phone, email & home address)	Back-up name & position	Back-up contact (office & cell phone, email & home address)
BCP Chairman				
Programs (2-3 Representatives)				
External Communications				
Human Resources & Staff Health				
Finance				
IT / Telecom Unit				
Logistics				
Security				
Organizational Development				
Volunteer				

Annex 1.3: Key contact numbers – Critical Response Management Team

Department represented	Critical staff name & position	Critical staff contact (office & cell phone, email & home address)	Back-up name & position	Back-up contact (office & cell phone, email & home address)
SG's Office:				
Finance and Accounting:				
Human Resources:				
Disaster Response Management:				
Health Service:				
Information & Communication Technology:				
Volunteer Management:				
Security Management:				
Logistics & Procurement:				
Internet & Web-Site Management:				
External Information & Communication				

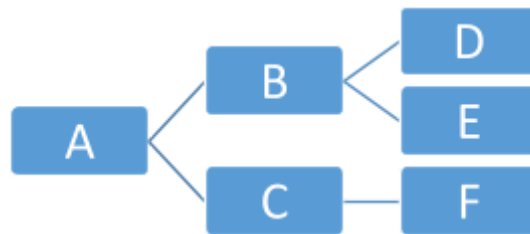
Office Equipment & Supply Management				
Vital Records Management:				

Annex 1.4: Key contact numbers – Critical Incident Staff

Department represented	Name & Position (Lead)	Contact (office & cell phone, email & home address)	Back-up (name & position)	Back-up contact (office & cell phone, email & home address)
NS leadership / CMT Lead				
Program teams (2-3 representatives)				
Communications unit				
Human Resources & staff health				
Admin Unit				
Finance Unit				
IT / Telecom Unit				
Logistics Unit				
Security Unit				
Organizational Development Unit				
Volunteerism / Youth unit				

Annex 1.5: Key contact numbers – NS Staff Phone tree

Please insert here corresponding NS Staff Phone tree, e.g.:



Annex 2: Critical function considerations

Critical functions
SG's Office -Provide strategic and operational leadership -External and internal coordination -Final decision making -Update the board and partners regularly -Ensure there is an alternative signatory for financial transactions -Chair the task force -Ensure effective risk management of the COVID-19 operation
Finance: -Ensure provision of timely cash flow to support all phases -Initiate payments -Review and approve requisitions -Approve LPOs -Approve accountabilities and adherence to donor conditions -Approve payments -Write reports -Perform bank Reconciliations -Ensure effective risk management of the COVID-19 operation
Disaster Management: Support to Health Department -Regular update of the IFRC.GO platform -Request for surge support -Coordinate with OPM depending if phase 3 -Co-chair the task force -Operational Movement coordination outside the country -Ensure effective risk management of the COVID-19 operation
Health: -Act as secretarial for task force -Regular situation updates to staff, volunteers and PNS' -Ensure guidance and support for critical field operations (EVD and COVID-19) with emphasis on safety for staff and volunteers. -Ensure coordination with MOH and other partners. -Ensure coordination of internal TRCS taskforce -Co-chair the task force -Ensure effective risk management of the COVID-19 operation
Human resources: -Ensure continuity of utilities and services. -Ensuring structured communication to staff especially if some staff must be asked to take unpaid leave -Check, monitor and comply with notification/obligations required by the Government and make all appropriate containment, isolation or quarantine arrangements. -Ensure all staff can access medical treatment during this time -Ensure medical services are up and running -Ensuing security of the TRCS premises -Ensuring cleaners and disinfectors are available daily -Sending relevant communication to staff -Provide support in terms of recruitment of the COVID-19 emergency response -Set up the documents for hardship allowances when possible -Ensure effective risk management of the COVID-19 operation

- plan cleanness and disinfection of office spaces
Communications and PR:
-Coordinate with task force for standardised messaging -Ensure dissemination of developed messages to all stake holders through the defined communication channels. -Update Social Media platforms with TRCS COVID-19 activities -Design visual messages for dissemination -Constitute a crisis communication team. Offer key messages for Public information. -Respond to media and public inquiries and offer lifeline communication to affected sections of the Public -Ensure effective risk management of the COVID-19 operation
PMER:
-Ensure development of tools for reporting on COVID-19 response. -Manage consolidation of reports -Integrate reporting on COVID-19 in National Society reports. -Support proposal development for resource mobilization. -Ensure effective risk management of the COVID-19 operation -Development and updating EPoA
OD & volunteer management
-Support & work with Branches to identify and deploy Volunteers as required. -Follow up Branches to ensure that measures are put in place against COVID-19 as per guidelines. -Support communications to Branches about COVID-19 response. -Ensure well-being and safety of volunteers in line with movement duty of care protocols. -Ensure all volunteers are insured and receive timely their incentives -Ensure effective risk management of the COVID-19 operation.
Audit:
-Reviewing the reliability and integrity of financial and operating project information -Reviewing, appraising and reporting on the economy and efficiency use of project resources. -Reviewing the project operations to ensure results are consistent with established objectives and goals. -Ensure effective financial risk management of the COVID-19 operation
Logistics and Procurement:
-Logistics support -Support procurement and supply chain
ICT:
Support ICT services

Annex 3: Terms of Reference example – Critical Response Management Team (CRMT)

1. Composition and activation

Total 7 members

- One Director each from Disaster Management, Health, Communication Departments, Deputy Secretary General, Secretary General and President
- If Director is unable to participate, nominate a deputy director or person in advance (during non-disaster times)
- Meetings should be convened with minimum available participation i.e. at least three members
- Members are appointed by position
- Other department representatives to be invited as deemed appropriate by the Chair
- Chaired by the President (back up chair – Secretary General) and Deputy Secretary General Programmes is the Secretary of the CRMT
- Meets every day at Emergency Operations Center (EOC) after activation
- Operations Manager to be supervised by the Secretary of the CRMT (the Deputy Secretary General Programmes)
- Activated by the President
- When the recovery phase starts, the CRMT will continue to supervise the Operation

2. Roles and responsibilities

Overall role is as a decision-making body once activated.

Responsibilities (related to ACTION):

- Declare the level of Emergency (small, medium and large-scale) or a possible emergency based on early warning information available
- Activate the NS EOC
- Activate the Emergency Finance and Logistics Procedures including usage of Emergency Management Fund
- Conduct a Safety and Security Assessment⁵ and implement necessary measures
- Take decisions regarding use of global tools (DREF, APPEAL, RFL POOL, FACT, ERU, RDRT etc.)
- Guide the preparation of a possible deployment of RCVS from other townships/states/regions (Regular, ERT, NDRT, ECV and RFL-trained)
- Activate the Staff HR roster⁶
- Appoint and supervise an Operation Manager (OM) who will be the lead in the early warning phase and thereafter the response and recovery operation (if needed)
- Approve the Response Plan of Action (including budget)
- Authorize Appoint media focal point/s

⁵ Safety and Security Assessment guidelines to be developed by Safer Access team

⁶ A roster to be developed for staff deployment during disaster

Responsibilities (related to OVERSIGHT)

- Stand by local NDRT & ERT, ECV-trained and RFL FP RCVs to assist local authorities in evacuation if needed
- Ask for an update/check on inventory readiness and condition of all relief stockpile and stock balance in the warehouses for all sectors, including stock supported by Movement partners, vehicles, transport providers at all levels and pre-agreements with suppliers reviewed

Annex 4: Terms of Reference example – Operations Response Team (ORT)

1. Composition and activation

- o Total 10 members
- o ORT led/managed by Deputy Secretary General Programmes and OM is the Secretary of the ORT.
- o One Deputy Director from Disaster Management, Health, Communications, RFL, Finance, Resource Mobilization, PMER, Logistics, OD, HR;
- o Deputy Director to nominate a Program Coordinator or other representative if unavailable;
- o Other department representatives to be invited as deemed appropriate by the Operations Manager.

2. Operations Manager

- o ORT members to act as a liaison with their respective department manager and provide information to OM as needed/requested;
- o Supported by EOC staff;
- o EOC staff to be managed by Operations Manager while ORT is active and by DM director during normal time.
 - One Deputy Director from the ORT to represent NS at the national EOC on a rotating basis; one week per Deputy Director
 - Deputy Director to be supported by one EOC officer who will be in EOC till the dissolving of ORT.

Activated by the CRMT:

- o Deputy Secretary General Programmes reports to the CRMT on daily basis
- o Meets every day after EOC is activated. Work from the EOC
- o Dissolved at the beginning of recovery period
- o When the recovery phase starts, the Deputy SG will continue to supervise the OM and to coordinate with the respective Department.

3. Roles and Responsibilities:

3.1. Initial response (0-1 week):

- o Prepare and review daily plan of action
- o Coordinate and ensure timely deployment of RCVs - Regular, ERT, NDRT, ECV-trained (from other townships if needed) - to assist local authorities in life-saving operations, first-aid provision, water, sanitation promotion, support referrals & medical evacuations, quarantine, relief distributions, evacuations and RFL services.
- o Ensure provision of first aid to injured patients and support referrals and support medical evacuation.
- o Support coordination with local life-saving operation (First Aid, referral and dead body management) for mass causality.

- o In case of quarantine, coordinate and ensure timely deployment of volunteers trained in ECV, PHiE, WatSan & First Aid
- o For RFL services, deploy RFL focal persons or RFL-trained volunteers
- o Prepare daily progress information (based on data collected from branches and its analysis) for CRMT updates and undertake necessary actions as advised by the CRMT
- o Ensure daily finance management including system of collecting locally donated funds
- o Provide daily financial updates to CRMT

3.2. Rapid assessment (0-2 weeks)

- o Identify the most-affected areas for conducting rapid needs assessment (DANA) and prepare rough plan of action. Coordinate with other actors (e.g. OCHA) and decide for joint (or) complementary rapid assessment
- o Deploy and organize RCVs, ERTs and NDRTs for rapid assessment with sectorial specialists in coordination with G1
- o Send surge support from NHQ staff to most-affected areas/townships
- o Conduct rapid assessment using the rapid assessment. Assessments should have a multi-sectorial perspective. (For health epidemics, Deputy Director, health is responsible)
- o Analyse the information from assessment reports and submit assessment report to CRMT

3.3. Response (1-2 weeks)

- o Guide and coordinate immediate relief assistance (e.g. relief kits, Hygiene Kit, safe delivery kits, WatSan material, SAR, FA, Shelter tool kits. RFL services. etc.) carried by the branches at local level in coordination with local actors (e.g. RRD)
- o Produce daily information report on the distributions done encompassing all sectors.
- o Share reports with national EOC, UNOCHA and other actors daily.
- o Analyze/process the findings from rapid needs assessment (all sectors), draft an assessment report and a Response Plan of Action until week 4 with budget.

3.4. Response (1-2 weeks)

- o Ensure information is disseminated to community at regular intervals including information on: NS, the response, access to services, and wider information needs as identified in assessment
- o Implement Response Plan of Action by mobilizing relevant resources such as:
- o Mobilize ERT/trained RCVs with required expertise based on plan of action (FA, PSP, RFL, WatSan, PHiE, Logistic, Shelter)
 - Make the logistic/procurement requisition by sector according to plan of action
 - Continue to ensure distribution of relief items and carry out sector-specific response according to Response Plan of Action.
 - Activate beneficiary feedback mechanism and ensure community is oriented on

3.5. Continued response (2-4 weeks)

- o Continue implementation of Response Plan of Action and conduct monitoring of operations
- o Implementation of planned activities and revision of plan of action (> 4 weeks)
- o Conduct detailed sector-specific assessments to feed into the Recovery Plan of Action in coordination with other actors.
- o Compile an operation update at the end of 4 weeks to share information on the situation and response so far.
- o Develop a Recovery Plan of action based on analysis of detailed sector-specific assessment reports, beneficiary feedback and monitoring of operations.
- o Continue response operations

3.6. Recovery Operation:

- o Roster of Operations Manager to be developed
- o Roster opened to all NS departments from whom the applications will be received and best candidates will be selected for the roster
- o Operations Manager selected by CRMT from the roster
- o Operations Manager duration to be decided by CRMT in consultation with HR (OM position may be responsible to lead recovery operations and recovery team)
- o Department from where OM is appointed needs to be supported to carry out the regular duties of the department
- o Operations Manager is accountable to the CRMT

Role and Responsibilities:

- o Participate in daily meetings with CRMT and update CRMT on behalf of ORT
- o Conduct staff recruitment at levels for the response operation, as needed
- o Lead the ORT and ensure its activities are carried out including initial response, rapid assessment, implementation of response plan of action, monitoring of response plan of action
- o Manage the ORT members and all response structures/teams set up or activated for the response
- o Maintain the relationship with CRMT and update the CRMT regularly
- o Ensure relevant finance management documents including budgets are prepared and have necessary approvals
- o budget development process and review
- o Monitor budget utilization and ensure appropriate budget utilization levels
- o Ensure compliance of relevant HR regulations
- o Carry out internal coordination with all departments
- o Develop and maintain relationship with external actors and ensure coordination
- o Ensure timely and effective narrative and finance reports are available
- o Coordinate with internal and external stakeholders

Annex 5: Emergency Operations Centre functions

Please insert here corresponding NS EOC functions.