Business Continuity Management User Guide

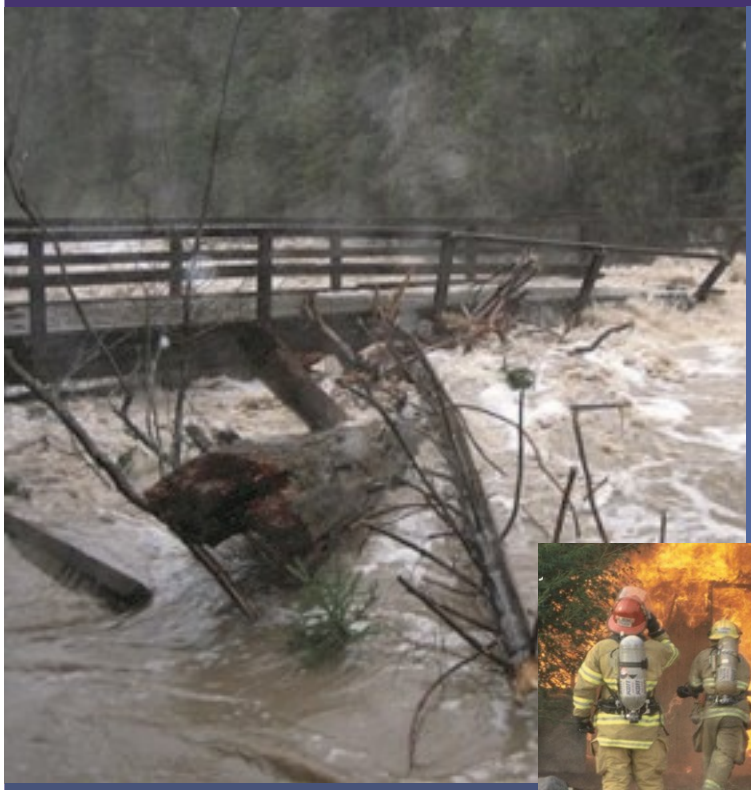


Table of Content:

Preface:

This User Guide provides an operational framework to ensure that critical decisions and actions are taken quickly by UNDP New York and Country Offices in crisis situations. It is intended for UNDP staff who have a specific role assigned within the context of Business Continuity.

During crisis management, regional hubs and policy centers should work closely with UNDP CO Resident Representative, Regional Security Advisor, Security Management Team, Department of Safety and Security (DSS) and follow Designated Official (DO) advise as required. If a regional Hub or Policy Center is embedded within a UNDP CO, then one BCP should include cover both offices.

The guide takes the reader through Standard Operating Procedures for Crisis Management and the essential elements in a Business Continuity Plan.

Users are welcome to send feedback and comments to Nesreen Al-Hebshi, nesreen.alhebshi@undp.org

A) Standard Operating Procedures for UNDP Crisis Management in New York

1. The aim of these Standard Operating Procedures (SOPs) is to provide an institutional and operational framework so that critical decisions and actions can be taken quickly and effectively by UNDP New York in crisis situations.

2. The SOPs apply to all UNDP administered personnel in New York involved in the various stages of Crisis Management.

3. The SOPs detail the roles and responsibilities of personnel involved in the three phases of UNDP New York crisis management activities, namely:

   I. Preparation;
   II. Emergency response (including crisis communication);
   III. Continuity of critical functions and operations (including business resumption).

4. In UNDP, the Security Management Group (SMG) is the operational body which oversees and implements the HQ crisis operations and security plans and serves as the Crisis Management Team for HQ emergencies and crises. The SMG consists of Directors or Deputy Directors of essential operational business units and is chaired by the Associate Administrator.

5. It is important to note that UNDP New York crisis management includes interaction with other UN agencies based in New York as well as with two UN entities, namely: The Senior Emergency Policy Team (SEPT) and the Crisis Operations Group (COG).

6. The SEPT is responsible for any policy required to deal with any given crisis. Examples of decisions that may be required are: continuation of scheduled UN meetings, suspension of routine operations, relocation and evacuation of staff and offices, or/and formal requests to the host country.

7. The COG consists of personnel from key administrative and support functions. It is chaired by the Under-Secretary General (USG) of the Department of Safety Security (DSS) and is responsible for operational decisions and their implementation in line with the policy directives of the SEPT.

I. PREPARATION

Security Management Group/Security office

8. The mechanism established for crisis management in UNDP New York is the Security Management Group (SMG). As such, responsibility for crisis management in New York rests with the SMG. The SMG consists of Directors or Deputy Directors of essential operational business units and is chaired by the Associate Administrator or BMS Director.

9. Under the direction of the Chair of the SMG, and in consultation with UNDSS, the Security Office develops a Security Plan and Crisis Management Plan, which includes emergency response, crisis communications, ITDR, continuity of critical operations and resumption of normal operations. The Crisis Management Plan will assist in managing and resolving emergency situations. The Chair of the SMG should ensure that the various elements of the plan are tested regularly to ensure that they are realistic and can be implemented in an actual situation.

II. EMERGENCY RESPONSE (0-12 Hours)

10. If a crisis situation occurs, the Administrator, Associate Administrator or BMS Director will represent UNDP at the SEPT and will inform the Director of BMS of any policy directives issued by the SEPT. BMS Director, the Director of Office of Operations, Legal and Technology Service (OOLTS), or delegated authority will represent UNDP at the COG and will ensure that response activities in UNDP are implemented in line with SEPT policy directives and COG recommendations.

11. The Associate Administrator then convenes the SMG to assess, with UNDSS collaboration:

    a. Threat to staff and their dependents;
    b. Damage to and accessibility of the buildings;
    c. Damage to other organizational assets;
    d. Ensure the availability of information and communication technologies;
    e. Update the list of key partner, vendors and suppliers;
    f. Impact on staff locations: NY City, NY State, NJ, CT, DC and PA.

12. If the SMG assessment does no conclude that staff, other organizational assets, ICT key partners, or vendors and suppliers are affected, the SMG informs the Administrator accordingly and business will proceed as usual.

13. If the SMG assessment concludes that there is a threat to the safety and security of staff and their dependents:
    1. The Chair of the SMG recommends that activation of the Crisis Management Plan (CMP) and appoints a Crisis Management Team (CMT) (consisting of selected members of the SMG, depending on the nature of the crisis). The CMT collaborates with UNDSS and is responsible for managing the crisis on a 24-hour basis until the resumption of normal operations.
    2. The Chair of the SMG activates a duty roster, enabling 24/7 operations of the Crisis Operations Center.

3. Within the Inter-Agency Security Management Network (IASMN) accountability framework, the Director of SO will position a liaison at the DSS CCC. The Chair of the SMG activates the UNDP Security Plan and recommends activation of the Crisis Communications Plan (Communications Office, Partnership Bureau).
4. The Crisis Management Team (CMT) oversees the execution of the Security Plan in UNDP.
5. The CMT in close coordination with the SO:
    a. Prioritize support to affected UNDP personnel and their families to maximize staff safety and security, including evacuation;
    b. Identify, coordinate and follow up with other UN institutions and agencies, e.g. with UNDSS on security issues.
6. The Chair of the CMT provides hands-on management of the emergency response on a full-time basis.
7. The Chair of the SMG maintains full-time communication with the Administrator and the UNDSS.
8. The Chair of the CMT coordinates required resources.
9. The Chair of the CMT maintains a log of all requests, actions and instructions, both given and received.

14. The Crisis Management Team will operate from the Crisis Operations Centre, a secure location prepared for rapid activation in an emergency situation. The location is equipped with adequate communications systems and houses copies of the CMP, the Security Plan, including the UNDP staff lists and evacuation maps, the Crisis Communications Plan, as well as the Business Continuity Plan, which should identify time sensitive functions to be recovered in order of priority, and the staff, resources and vital records required for their recovery.

III. CONTINUITY OF CRITICAL FUNCTIONS AND PROCESSES (12 hours - 3 months)

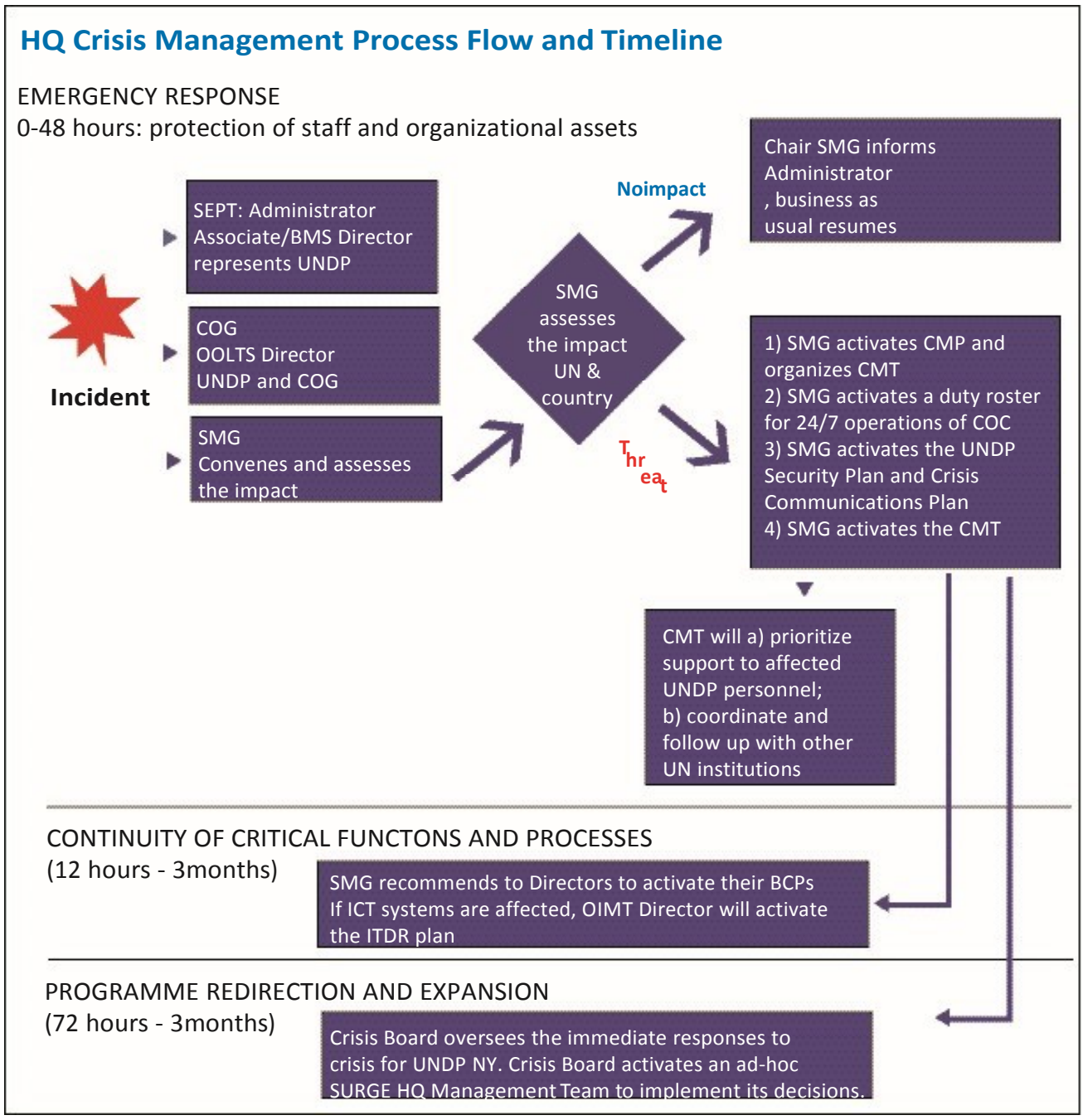
BMS Director, Regional and Units

15. SMG assessment concludes that availability of staff, other organizational assets, ICT and key partners, vendor and suppliers (or a combination of those) are affected and recommends activation of Bureax and Units' BCPs:
    a. Once all staff has been accounted for, the Chair of the SMG recommends that Bureaux/Units Directors activate their BCPs;
    b. If the organization's information and communications system are affected, the Chief of OIMT will immediately activate the ITDR Plan. The Chair of the SMG maintains full-time communication with the Administrator;
    c. The Chair of the CMT oversees the execution of the Business Continuity Plans. The CMT maintains a log of all requests, actions and instructions, both given and received.

Debriefing

16. After the crisis is over and all business units return to normal operations, a review and evaluation of the Security and Business Continuity Plans should be conducted by the Security Office, OIMT, BMS and all other business units. The review should include recommendations concerning modifications to the Plans. This will enable the respective owners to make improvements to their Plans. Copies of evaluation reports must be forwarded to the Chair of the SMG.

1- Crisis Management Flowchart HQ



17. The aim of these SOPs is to provide an institutional and operational framework so that critical decisions and actions can be taken quickly and effectively by UNDP Country Offices in crisis situations.
18. The SOPs apply to all UNDP administered personnel in New York involved in the various stages of Crisis Management.
19. The SOPs identify decisions and actions in four phases of crisis management and response, namely:

    I. Preparation;
    II. Emergency response (including crisis communication);
    III. Continuity of critical functions and operations (including business resumption);
    IV. Programme redirection and expansion.

I.PREPARATION

Designated Official/ Resident Representative

20. The mechanism established for crisis management at UN duty stations is the UN Security Management Team (SMT) headed by the Designated Official (DO) for security. As the coordinator of the UN system, UNDP supports the DO function through inter-agency mechanisms established in-country. The composition of the SMT depends on the size of the UN Country Team (UNCT) and the agencies present. It will include the DO, the Heads of Agencies, the Field Security Officer, and appropriate resource persons as required by local conditions, such as: a medical officer, an internationally recruited staff member familiar with local conditions and/or the local language, and a communications officer. Under the direction of the DO, the SMT develops a Crisis Management Plan (CMP) which will assist in managing and resolving emergency situations. The DO should regularly test the various elements of the plan to ensure that it is realistic and can be implemented in an actual situation.

21. The UNDP Resident Representative, if acting in capacity as DO, ensures that the UNCT has updated and actionable Security and Contingency Plans. The UNDP Resident Representative, as Head of Agency in-country, should ensure that the CO has updated and actionable Security and Business Continuity Plans.

II. EMERGENCY RESPONSE (Protection of staff and organizational assets: 0-48 hours)

Designated Official

22. If acting in capacity as DO, the Resident Representative (RR) convenes the SMT to assess:
    a. Staff/personnel safety and security;
    b. Threat to staff and their dependents;
    c. Damage to and accessibility of the building;
    d. Damage to other organizational assets;
    e. Availability of information and communication technologies;
    f. Availability of key partner, vendors and suppliers;

g. Impact on the country.

UNDP

23. The RR analyses the same elements as above for UNDP staff, premises and assets. The RR informs the RB Director and the Director of the Security Office.
24. If SMT assessment concludes that no staff, other organizational assets, ICT and key partners, vendors and suppliers are affected: The RR informs the RB Director and the Chief of the Security Team accordingly and business will proceed as usual.
25. If SMT assessment concludes that there is a threat to the safety and security of staff and/or their dependents.

SMT:

26. The DO activates the CMP and organizes a UNCT Crisis Management Team (CMT)*. The composition of the CMT is determined by the DO in consultation with the SMT. SMT members are selected for the CMT based on the nature of the crisis and the subject matter expertise required. The CMT is responsible for managing the crisis on a 24 hour basis until the emergency is resolved. The CMT meets daily as required to provide coordinated control among and communications between all entities involved in the crisis (including, amongst others, the host government, heads of agencies in country and headquarters locations).

UNDP

a. The RR activates the UNDP Security Plan which includes specific Contingency Plans, as required (e.g. Pandemic Preparedness).
b. The RR activates the UNDP Crisis Management Team (CMT)*, which consists of critical programme and operations personnel, to oversee the execution of the Security and Business Continuity Plans for UNDP in-country.
c. The RR informs the RB Director and the Director of the Security office that the Security and Contingency Plans have been activated.
d. The RB Director convenes the HQ Crisis Board to:
    a) prioritize support to affected UNDP personnel and their families to maximize staff safety and security, including evacuation and safety corridor arrangements for national staff;
    b) identify, coordinate and follow up with other UN institutions and agencies, e.g. with UNDSS on security issues.
e. The CMT provides hands-on management of the emergency response on a full-time basis.
f. The CMT maintains continual communication with the HQ Crisis Board.
g. The CMT coordinates required resources.
h. The CMT keeps the RR fully informed at all times.
i. The CMT maintains a log of all requests, actions and instructions, both given and received.
j. The UNDP Crisis Management Team will operate from a secure location prepared (wherever applicable) for rapid activation in an emergency situation. The location should be equipped with adequate communications systems and should house copies of the CMP, the security plan, contingency plans - including the UNDP staff lists and evacuation plans and maps, as well as the business continuity plan, which should identify time sensitive functions to be recovered in order of priority, and the staff, resources and vital records required for their recovery.

III. CONTINUITY OF CRITICAL FUNCTIONS AND PROCESSES

Resident Representative/UNDP Crisis Management Group/HQ Crisis Board

27. SMT assessment concludes that availability of staff, other organizational assets, ICT and key partners, vendor and suppliers (or a combination of those) are affected and recommends activation of Agencies' BCPs:
    a. Once all staff have been accounted for, the RR activates the BCP, including the IT Disaster Recovery and business resumption plan (if necessary) and informs the RB Director and the Director of the Security Office accordingly;
    b. The CMT oversees the execution of the Business Continuity Plan;
    c. The CMT maintains a log of all requests, actions and instructions, both given and received;
    d. The HQ Crisis Board coordinates operational support measures and mobilizes immediate responses from relevant HQ units for CO.

IV. PROGRAMME REDIRECTION AND EXPANSION (72+ hours) UNDP Crisis

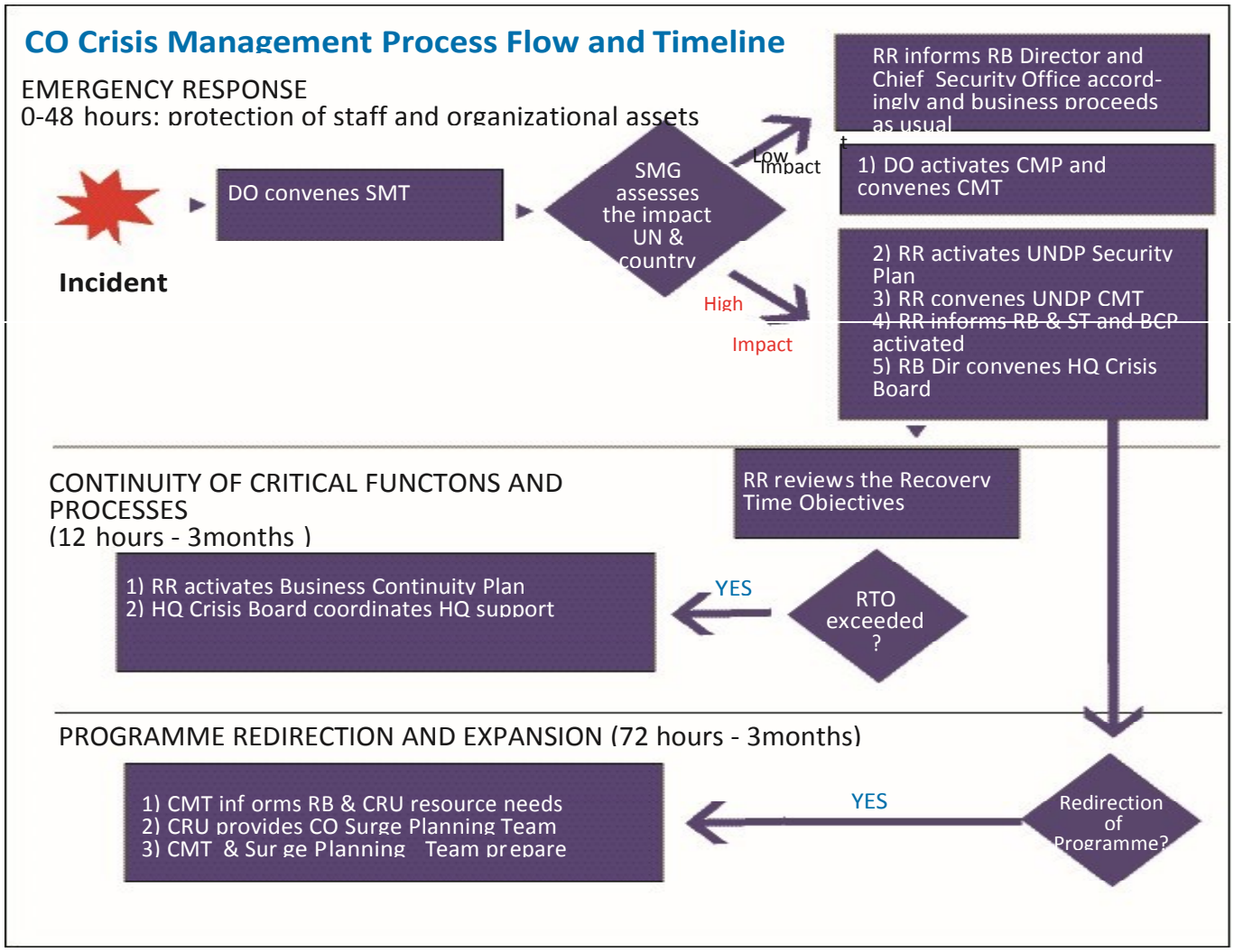
Management Team/RB/CRU

a. Upon reestablishment of critical functions and processes, the CMT will inform the RB and CRU of their resource needs in order to prepare a SURGE Work Plan
b. CRU will provide the CO with planning support - the SURGE Planning Team - which is deployed to the affected country by the end of the first week after the onset of the crisis event.
c. The CMT and the SURGE Planning Team prepare the SURGE Work Plan, which defines UNDP's response to the crisis in the first three months.

Debriefing

28. After the crisis is over and the CO returns to normal operations, a review and evaluation of the Security and Business Continuity Plans should be conducted by the CMT. The review should include recommendations concerning modifications to the Plans. This will enable the RR to make improvements to the Plans. A copy of any evaluation report prepared by the CMT must be forwarded to the RB Director and BMS and will be copied to the members of the HQ Crisis Board.

Crisis Management Flowchart CO



Main Procedures of Business Continuity Plan

No.	Steps	Responsible Party	Template/Guidelines	Explanatory Note
1	Prepare/Review/Update CO/Unit **Security Risk assessment**.	BCP focal point	Risk Assessment Template	This includes Country Risk Assessment which is prepared by DSS in consultation with the SMT Reference is DSS Country Risk Assessment Assessment should be annexed to BCP
2	Prepare/Review/Update CO/Unit **Business Impact Analysis**.	BCP Focal point	BIA Template	This means identification of critical business functions and assessment of impact from identified risks along with recovery time Objectives of critical functions along with necessary ICT tools/equipment to continue these functions Identify essential CO documents; keep hard and soft copies in off-site location/onedrive This is a collective exercise that is done in consultation with Senior Management Assessment should be annexed to BCP
3	Prepare/review/update CO/Unit BCP Document	BCP Focal	CO BCP Template HQ BCP Template ICT Disaster Recovery Plan Template	Based on the Risk Assessment and BIA, review/Update existing BCP to ensure inclusion of most recent critical function, critical staffing list with alternate and their contact details Pre-identify off-site location to ensure that in the event of an emergency, CO/Unit can operate from. Necessary power and ICT connectivity is essential (e.g working from home, working from another agency office) ICT Disaster recovery plan to be prepared
4	Share draft BCP with all supporting doc with BMS Directorate	BCP Focal point		Via email
5	BMS Directorate review and provide CO/Units any comments	BMS BCP Specialist		Via email
6	Approve/sign off BCP Doc	Head of Office		All supporting docs are to be annexed in the

7	Arrange for BCP Test	Head of Office	BCM User Guide	BCP simulation Exercise should test the Viability of identified critical functions and procedures the way they would be performed in a real crisis/critical incident. The test can access CO's crisis management plan, business continuity plan, and ICT disaster recovery plans. Lessons learnt should be drawn from the Exercise and modify BCP as necessary.
8	Upload signed BCP and BCP Test report	BCP Focal point	BCM Site	

29. Other important elements for BCP consideration include the following:

    a. Prepare Order of Succession plan
    b. Identify Chain of communication/communication tree/warden system
    c. Ensure Accessibility of personnel contact lists
    d. Ensure MOSS compliance
    e. Ensure availability of updated list of other agencies/offices located outside the building
    f. List of Government, donors and key stakeholder names and numbers
    g. Ensure availability of updated List of Critical staff/functions
    h. Ensure accessibility of Medical support local & international List - Authorities
    i. Access to cash (in coordination with OFM)
    j. Travel/Logistics support
    k. Security Safety Procedures- Staff Contracts
    l. Off-site location
    m. Assembly points are identified and known to all personnel and wardens
    n. Availability of trauma and first aid kits
    o. Pre-identify potential crisis management Team members

BCP Testing and Exercise:

30. According to the BCM policy, BCP should be tested at least once a year. Testing and exercising is part of the overall BCM to ensure Business Continuity Preparedness, office capability to implement the plan and to familiarize personnel with the process should a crisis happen. BCP simulation Exercise should test the viability of identified critical functions and procedures the way they would be performed in a real crisis/critical incident. The test can access CO's crisis management plan, business continuity plan, and ICT disaster recovery plans.

31. Testing should help COs/BU identify BCP deficiencies, clarify roles and responsibilities and access communicatio tools developed for the plan. The exercise can be a tabletop, incident simulation test or full simulation test. Lessons learnt should be drawn from the exercise and modify BCP as necessary.

BCP Testing Scenario - Sample
Date:

Test Objectives:

- To evaluate and **improve the capability of the team**, units and individuals in the country office to execute their emergency management and operational responsibilities;
- To **familiarize all staff**, especially those directly involved in BCP implementation with the Plan;
- **To Enhance the readiness of the office to respond to an incident**;
- To **assess and validate relevant plans, procedures, and systems**, and identify deficiencies for subsequent correction;
- To **test operability of the decision-making process**, including the setup and functioning of the Crisis Management Team (CMT);
- To **test the setup and functioning of alternative recovery site(s)**;
- To identify gaps in the BCP and areas of improvement for possible follow up actions.

Pre-requisites:

- Updated staff list/communication tree/warden system are in place;
- Off-site internet connectivity for staff to work remotely;
- Communications tools are available to Senior Management (mobile, Satellite mobile, BGAN, etc.).

BCP Test Scenario:

To be developed in line with the risk assessments and identified threats. Please contact BCM Management

Specialist in BMS for any assistance.

Scenario details (All emails/communications should include that this is a BCP exercise/test including emails sent to HQ)

	Time	Activity	Focal point	Successful (YES/NO)	Challenges	Recommendations
Testing Communications						
1	TBC	send an e-mail informing all staff/personnel of situation and BCP activation while Noting that the office is inaccessible and maybe affected	RR/CD			

2	TBC	inform HQ and devolution office (RBx and BCP focal point)	CD			
3	TBC	Accounting for staff: Warden to conduct warden check of all staff . Wardens must contact staff via landline/cell phone and report status of staff count to the Chief Warden and HQ	DCD and wardens			
4	TBC	Crisis Management Team to meet virtually to identify critical functions and operations after which critical staff are informed (minimum operations to be selected)	DCD/ICT			
	TBC	DCD requests ICT to confirm that all connectivity is operational and that up-dated back-up is in alternate location.	OM			
5	TBC	Continue to get regular SITREPs and disseminate them to staff. UNDP's server incapacitated and alternative e-mail addresses used to distribute a test message. All staff to confirm receipt via return message	CD			
Testing Critical Processes						
Simultaneous Testing Travel/logistics						
		Due to the crisis, BRx decides to send surge capacity – Regional Security Advisor				
6	TBC	DCD requests travel Unit to initiate travel process Request travel information and proceed with securing visa and DSA payment	OM/ travel			
7	TBC	Due that crisis, it is found that travel agent system is down and cannot provide the service and devolution	DCD/OM			

		country office has been asked to support to finalize travel arrangement including approval				
8	TBC	DO has to attend an urgent meeting with national security authority and transportation is required	OM/admin/ driver			
HR Processes						
		Due to crisis, considering that the crisis may be prolonged, RR requests crisis management team to check on staff HR issues	RR			
9		HR to check in Atlas that all FTA, SC and IC contracts are up to date, reporting back to CD and DCD	OM/HR			
10		HR to check with Copenhagen to prepare procedures for evacuation of international staff and ensure that all staff contracts are in order	OM/HR			
DR ICT Processes						
11		Check functionality of wireless modem devices to provide internet connectivity. Ensure staff have either batteries, solar chargers or car plug in chargers to power devices in the event of a power outage.	OM/ICT			
12		Check functionality of satellite phones to provide telephone connectivity both within country and to destinations outside of country.	OM/ICT			
13		Retrieve, mount and view data from tape backups to view shared files	OM/ICT			

	14		Review documentation for ICT licenses, software libraries, ICT architectures, system diagrams, technical documentation, encryption keys and safe combinations. Ensure you have sufficient information to completely reconstitute ICT infrastructure in the event of a catastrophe.	OM/ICT			
Conclusion of BCP Test Exercise							
	15		send a broadcast email to all staff, informing that the BCP test has now concluded, and that full operations have been restored.	CD/DCD			
	16		Upon the conclusion of the BCP test exercise, the CMT members will consolidate their detailed notes on all actions to report lessons learned meeting on the following day.				