


## Administrative Instruction

Date: 16 April 2010  
To: All UNOPS Personnel  
From: Karsten Bloch  
Director, Corporate Support Group 

AI Reference: AI/CSG/2010/01  
Subject: **Business Continuity Planning and Disaster Recovery Framework**

### 1. Introduction

1.1. In accordance with section 16(p) of UNOPS Strategic Risk Management Planning Framework (Organisational Directive No. 33), I hereby promulgate AI/CSG/2010/01 on “UNOPS disaster recovery and business continuity planning framework” (attached).

### 2. Purpose

- 2.1. The purpose of this Administrative Instruction (AI) is to establish the business continuity planning and disaster recovery framework for UNOPS headquarters and regional entities.
- 2.2. The overarching goal of this document is to help mitigate the risk posed in the event of a disaster in a UNOPS office by providing a framework of procedures, organisational structures and preparedness measures focused on the safety of personnel, the continuity of critical/essential services and functions and the liaison and coordination with local authorities, the UN system and other stakeholders.
- 2.3. This AI is designed to be implemented in conjunction with existing United Nations policies, practices and procedures and is subject to existing and/or forthcoming policies established/to be established by UNOPS Executive Director.

### 3. Transition measures

- 3.1. Each Regional Director shall ensure that each office under his/her supervision has a business continuity and disaster recovery plan (a template of which is provided as Annex I of this AI) by **31 December 2010**.
- 3.2. The said completed business continuity and disaster recovery plan must be uploaded on the intranet at:

<https://intra.unops.org/ToolsResources/SafetySecurity/UNOPS/Pages/UNOPSHQBusinessContinuityManagement.aspx>

### 4. Effective date

- 4.1. This AI is effective **1 May 2010**.

**ADMINISTRATIVE INSTRUCTION  
(AI/CSG/2010/01)**

**Pursuant to section 16(p) of Organisational Directive No. 33**

**BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY FRAMEWORK**

**1. Statement of a policy/framework**

- 1.1. As stated in the UNOPS Organisational Directive No. 33 (“UNOPS Strategic Risk Management Planning Framework”):

*“16. UNOPS approach to embedding its risk management system throughout the organization may include the following components:*

*p. Disaster recovery and business continuity planning – particularly addresses mitigation of operational risks associated with functions under the overall authority of UNOPS Corporate Support Group. CSG will develop and promulgate a Business Continuity framework detailing specific risks categories associated with facilities and infrastructure. The framework will, inter alia, clarify roles and responsibilities and provide practical tools for readiness assessment and contingency planning at relevant levels. Furthermore, special instructions on operating in an emergency situation may, as appropriate, be embedded in policy and guidance developed and issued by UNOPS Management Practices.”*

- 1.2. Hence, this AI is promulgated pursuant to section 16(p) of Organisational Directive No. 33.

**2. Objective and scope**

- 2.1. UNOPS recognises the potential strategic, operational and financial support risks associated with service interruptions and the importance of maintaining viable capability to continue UNOPS activities with minimum impact in the event of an emergency.
- 2.2. The objective of this framework is to formalize UNOPS business continuity and disaster recovery planning to establish the basic principles necessary to ensure emergency response, resumption and recovery, restoration and permanent recovery of UNOPS operations and activities during a business interruption event.
- 2.3. This framework also provides guidelines for developing, maintaining and exercising Operations Centre (OC)/Project Centre (PC)/project team bases-specific business continuity and disaster recovery plans.
- 2.4. This framework applies to all UNOPS personnel, facilities, infrastructure and IT systems at all UNOPS offices, throughout the world. UNOPS offices shall be prepared for scenarios and including, but not limited to, political instability or event, natural disaster,

power outage, hardware/telecommunications failures, data corruption, explosives and chemical, biological and nuclear hazards (any unplanned event, occurrence or sequence of events that has a specific undesirable consequence). These events may be local in nature, rendering only a single office facility inaccessible, or could have regional impact, with multiple offices facilities in a geographic region becoming inaccessible.

### **3. UNOPS-wide Business Continuity and Disaster Recovery Plan (BC/DRP)**

- 3.1. CSG shall develop the institutional BC/DRP from an international crisis. Recovery plans for business functions and systems with UNOPS-wide impact shall be the responsibility of CSG and be addressed in the UNOPS-wide BC/DRP.

### **4. Regional/local BC/DRP**

- 4.1. The BC/DRP for a regional/local crisis and recovery of critical processes shall be developed by the respective OC Director/PC Manager/Project Team Base Project Manager together with the relevant Regional Director, and consistent with the area Security Management Team, the UN Designated Official and the Security Risk Assessment. However, CSG shall provide assistance/support, if required, in the creation of regional/local plans to provide leadership and guidance, and ensure appropriate consistency and coordination among the various regions, as well as compliance with this AI.
- 4.2. The regional/local BC/DRP must be based on a risk assessment that considers potential losses due to unavailability of service versus the cost of resumption. These plans shall anticipate a variety of probable scenarios.
- 4.3. UNOPS Regional Directors (RDs) have the responsibility to ensure that regional/local BC/DRPs are prepared for the region and countries under his/her supervision, using the template attached herewith as Annex I.

### **5. BC/DRP contents**

- 5.1. A BC/DRP is intended to serve both as a working plan for achieving readiness and as guidance tool for response during a disaster.
- 5.2. The need for a comprehensive BC/DRP for each and every UNOPS office is essential. The objectives of the BC/DRP include the following:
  - (a) Safety of personnel. Reduce loss of life and minimize damage and losses and eliminate or mitigate the impact of disruptions on operations.
  - (b) Direct and guide appropriate actions to ensure the capability exists to continue critical processes and critical operational services.
  - (c) Achieve a timely and orderly recovery from emergency and crisis situations across a wide range of potential hazards with subsequent reconstitution of normal operations that allows the resumption of critical processes and operational services.

- (d) Ensure the succession of management, on a temporary basis, with accompanying authorities.
- (e) Liaison and coordination with local authorities, United Nations system and other stakeholders.
- (f) Protect and ensure access to essential facilities, equipment, vital records and assets.
- (g) Provide organizational and operational stability, by having the capacity to continue and control critical processes, operational services and functions until normal activities are reconstituted.
- (h) Facilitate decision-making during an emergency or crisis event.

5.3. Accordingly, BC/DRP for each office should:

- (a) Concentrate on providing guidance to ensure the capabilities to continue essential operations in the event of an emergency or when exposed to a broad range of risks. Under an all-hazards approach, preparedness measures shall be codified in the BC/DRP.
- (b) Define the roles and responsibilities of UNOPS personnel and specific actions to be taken by the individual offices in the event an incident disrupts the normal activities of the office.
- (c) Maintain current lists of all ‘essential’ and ‘critical’ personnel, including detailed plans to secure priority assets.
- (d) Include key security aspects. These must include at a minimum: established UNOPS safety and security policies and administrative instructions; procedures established by the respective country level UN Security Management System (UNSMS) including MOSS/MORSS requirements; and specific in-country security procedures/directives and alignment to the country security plan.
- (e) Include mandatory instructions, advice, process, procedure or guidance concerning internal and external communications.
- (f) Include technical measures that enable the recovery of information technology systems, operations, and data that is identified as critical.

5.4. BC/DRP should also reflect that following a disaster, the reconstitution of offices as a work place with adequate facilities and personnel to restore complete functions is a priority. Reconstitution operations may include actions to restore the primary warehouse facility to operational capability, or acquiring a new facility, working closely with other UNOPS, United Nations offices and the respective Governments, acquiring and installing equipment and communications, and redeploying personnel to the alternate site. Reconstitution sites may include other offices or those of other UN

agencies. The eventual establishment of an emergency relocation site at time of crisis, as is appropriate should be done in consultation with the Deputy Executive Director, respective Regional Director and UNOPS Chief of Security.

- (a) However, in some cases, it may not be necessary to redeploy personnel to another location. To address local crisis situations, alternate approaches for resumption including remote working from home may be identified.

## **6. Testing and updating of BD/DRP**

- 6.1. Each BC/DRP should be tested at least annually to ensure credible recovery preparedness. The scope, objectives, and measurement criteria of each test shall be determined and coordinated by CSG and the respective Regional Office.
- 6.2. Each BC/DRP must be regularly updated. Each office must report any changes, such as changes in personnel responsibilities, personnel contact information and/or functional changes to CSG.

## **7. Corporate communications**

- 7.1. External communication during time of crisis is a critical business process. CSG shall work with the Communication Unit to develop the process and messages that will be communicated to the personnel and to press in the event of a business interruption.

## **8. Training**

- 8.1. The respective UNOPS offices/OC Directors or PC Managers will ensure that all personnel are made aware of their responsibilities under their respective BC/DRP.
- 8.2. Each office/OC Directors or PC Managers is responsible for the training of personnel. The training of personnel is essential to ensuring each office maintains the capability to properly and efficiently execute its BC/DRP.

**ANNEX I****BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING**

OFFICE: .....

OC DIRECTOR /PC MANAGER RESPONSIBLE: .....

[This template gives a suggestion on how to structure a regional/local BC/DRP. It is not exhaustive and changes should be made to best fit the regional/local circumstances.]

The key contingencies that must be planned for clearly include:

- 
- 
- 
- 

It is vital that the plan is realistic and able to be implemented under scenarios that allow for the (realistic) provision of additional resources, and scenarios that utilise only current capabilities.

**Executive Summary**

- Outline of objectives
- Summary of contingency(s) and scenarios
- Prioritisation of contingencies
- Intervention strategy and planning summary

**Hazard and Risk Analysis**

*What hazards and risks to personnel, facilities and infrastructures exist?*

- Hazard and resulting risks analysis
- Risk mitigation strategies
- Challenges to particular units.

**Contingency for ...** [one for each contingency in multiple contingency plans]

*Disruption of services and affect on personnel safety, facilities, infrastructure based on hazard and risk analysis*

- Summary of contingency
- Brief summary of planning scenarios

**Scenario ...** [one for each scenario]

*Account of a possible course of events that could occur forming the basis for planning assumptions:*

- Scenario specific hazard and resulting emergency
- Likely triggers
- Scenario specific Risk Analysis
- Anticipated Duration of Emergency

**Contingency plan for ....** [One for each scenario and prioritised contingency]

*Details of how personnel will maintain prioritised operations and personnel safety based for each of the prioritised contingencies on scenario.*

**Response Strategy**

- Objectives of Proposed Interventions
- Appropriateness of Proposed Longer Term Relief and/or Development Activities
- Links to National plans and priorities
- Links to Country Team plans and priorities.

**Implementation**

- Immediate actions
- Needs Assessment of group identified in contingency
- Preparedness and response actions
- Monitoring and Reporting Arrangements
- Coordination Arrangements with National Authorities and other partners

**Resources: materiel required for interventions**

- Resources available
- Resources required
- Actions to provide identified resources

**Logistics**

- Transport
- Storage
- Telecommunications
- Security

**Internal management plan for business continuity**

- Decision-making Structure
- Triggers
- Coordination structures
- Personnel requirements
  - Critical personnel
  - Non-critical personnel
- Office and Sub-office Requirements
- Personnel Training and Guidance
- Security
- Media/Public Information Strategies

**Budget: estimated costs for preparedness and intervention**

- Direct costs
- Indirect, transport and other costs
- Support costs

## **Preparedness Actions and Plan Updating**

- Preparedness actions matrix: actions, status (complete, not-started, partially complete); responsible agency/individual and timeline.
- Response actions matrix: Triggering event; Action; Security Considerations; Personnel Actions.
- Testing of plan and preparedness
- Plan Update Schedule

## **Annexes and Attachments**

- List of UN and affiliated agencies present in-country
- List of Heads of Agencies and contacts
- List of critical PI personnel and alternates
- Security warden system (international and national staff)
- Responsibilities under the UN Security Plan (individual staff members and Heads Of Agencies)
- List of Area Security Coordinators (ASC) and Deputy Area Security Coordinators (DASC)
- Table of implementation/action points of the UN Contingency Plan
- Procurement and stockpiling list/overview
- Procurement costs per agency
- Communications plan