

UNDP Business Continuity Management Policy

(BCM)

**Executive Summary**

**Business Continuity Management (BCM)** is UNDP’s policy which sets the framework for the organization to respond to internal and external threats and ensures the organization’s preparedness, resilience and ability to continue delivering its mandate when such threats occur.

**BCM** in UNDP is in line with the **UN Organizational Resilience Management System (ORMS)** and acts as the emergency management framework for the organization. It includes the **IT Disaster Recovery Plan (ITDRP),** security plans (which include crisis, incident, and emergency management) and **Business Continuity Planning** **(BCP)**.

A **BCP** is based on a **Risk Assessment (RA) and Business Impact Analysis (BIAs)**. They build on existing Enterprise Risk Management policies and country-specific **Security Risk Assessments (SRA)** while considering the overall organizational mandate and continuation of business.

Table of Contents

[A. Background 3](#_Toc499038508)

[B. Objectives 3](#_Toc499038509)

[C. Risk Assessment 4](#_Toc499038510)

[D. Business Impact Analysis 4](#_Toc499038511)

[E. Business Continuity Plan 4](#_Toc499038512)

[F. Roles and Responsibilities for BCM 6](#_Toc499038513)

[G. Trigger for the activation of Business Continuity Plans 7](#_Toc499038514)

[H. Training, Exercising and Review 8](#_Toc499038515)

**UNDP Business Continuity Management Policy**

# Background

1. The safety and security of human populations is increasingly compromised by new or evolving threats, both natural and man-made. These include potential pandemics, extreme weather events or natural disasters, and often are interrelated threats from armed conflict, criminality, civil disorder and transnational terrorism. These threats imperil human lives as well as the stability of political, economic and social systems. As is the case with any multilateral institution, these events challenge UNDP to prepare and manage situations that may threaten the organization’s capacity and continuity.
2. UNDP is, therefore, corporately implementing a **Business Continuity Management (BCM)** policy, as part of an ongoing process of the current risk assessment and **Enterprise Risk Management (ERM)** policies, with the purpose of ensuring that the organization can continue to deliver its key services, while maintaining the safety and security of staff should a disruption or a threat arise. These risks can be external to the organization which UNDP has no control over, such as a power failure, or from within the organization, such as accidental damage to property.
3. The central elements of **BCM** in UNDP are incident management involving crisis/ emergency/disaster recovery (as reflected in the Security and Crisis Management Plans), crisis communications, IT Disaster Recovery Plan, and business continuity and recovery strategies for critical business functions, as reflected in the unit, bureau or country office **Business Continuity Plan (BCP).**

# Objectives

1. The aim of the **BCM** policy is to protect the interests of UNDP and its internal and external stakeholders by establishing a business-owned and business driven strategic and operational framework, which proactively ensures UNDP's ability to prepare and respond appropriately to anticipated risks identified within the context of a corporate risk assessment, unit level risk logs and any unexpected potential disruptive challenges, while maintaining staff safety and security.
2. **BCM** in UNDP is in line with the UN Organizational Resilience Management System (**ORMS**) and acts as the emergency management framework for the organization. It assists UNDP to build resilience by aligning and harmonizing preparedness efforts to enhance the organization’s ability to continuously deliver its mandate.
3. **BCM** complements Enterprise Risk Management (**ERM**), and provides tools to address those risks identified at office or unit level, which might impact the continuity of operations. BCM recognizes all existing activities and arrangements related to risk management, crisis response, and contingency planning, while it allows to:
4. Strengthen the ability of each country office to continue its business after the immediate response to an incident based on a thorough Risk Assessment (**RA**) and a Business Impact Analysis (**BIA**);
5. Interlink established structures and mechanisms for Risk Assessment and immediate incident response with activities necessary to ensure continuity of operations;
6. Determine the extent to which Business Continuity Planning (**BCP**) is necessary in each country office, based on the identified likelihood of incidents and the impact on staff safety and security and the continuity of operations, which differ significantly from country offices to country offices;
7. A Business Continuity Plan (**BCP**) is prepared after the Risk Assessment (**RA**) **and Business Impact Analysis** (BIAs) are conducted and concluded by the country office. These assessments build on existing Enterprise Risk Management and Country-specific Security Risk Assessments (**SRA**) while considering the overall organizational mandate and continuation of business.
8. Each Office/Unit must have a **BCP** Focal Point who should work under the direct instruction of the head of office/Unit.

# Risk Assessment

1. Under the oversight of the **Security Management Group (SMG),** a HQ Risk Assessment (bringing together Security and ERM) is carried out annually in collaboration with UN system partners. For UNDP HQ, the **Bureau of Management Services (BMS)** initiates discussions with partners in the UN Secretariat and in other UN agencies during the last quarter of each year to prepare a common Risk Assessment. Selected Security Office and **ERM** staff members work with colleagues of the UN, its agencies and with external entities as required on this. The outcome of the annual Risk Assessment is presented to the **SMG** and informs **BCM** decisions and planning for the subsequent year. Country Offices and Regional Hubs go through the same process at least annually but follow the cycle set according to prevailing procedures for updating their respective Security Risk Assessment (**SRA**) and Risk Logs.

# Business Impact Analysis

1. The Business Impact Analysis (**BIA**) is conducted by each country office or bureau unit, and coordinated by the office of the Business Continuity Focal Point. They may request technical assistance from the Directorate, Bureau for Management Services **(BMS**). The BIA includes:
2. Identification of the critical business functions,
3. Assessment of the impacts from identified risks that may disrupt critical business functions;
4. Specification of setting recovery times in the event of disruptions;
5. Defining recovery strategies for critical business functions, including the allocation of appropriate resources.

# Business Continuity Plan

1. Each office/unit must prepare and maintain a Business Continuity Plan (**BCP**), to ensure that the organization can carry out its functions, so far as is reasonably practicable, when faced with an emergency. The **BCP** must be reviewed annually.
2. At office/unit level, a Business Continuity Plan (**BCP**) provides:
3. A rehearsed method of restoring UNDP’s ability to maintain critical corporate and service level functions to the best possible standards, within a realistic time period after disruption;
4. A verifiable capability to maintain, test, implement, validate and audit **BCP**;
5. A pre-defined communication protocol to ensure all relevant units are aware of the **BCP** when activated.
6. At the organizational level, Business Continuity Management (**BCM**) provides:
7. Completed, implemented and tested Business Continuity Plans (including procedures for maintenance and monitoring), which reflect the determined extent of necessary preparations corresponding with the reality of each country office regarding critical incident exposure;
8. Stronger interlinked, as well as better informed and integrated, crisis response, risk management and business continuity structure and mechanisms in all UNDP country offices;
9. The ability to:

i) respond to an event so that staff safety and security is maintained,

ii) continue critical business functions with least possible limitations and/or interruptions, and

iii) regain full operational capacity as soon as possible after a disaster/crisis.

1. The **BCP** covers all UNDP-administered personnel, business functions at all levels, including those that have been subcontracted to external contractors and suppliers, where the overall legal responsibility remains with UNDP. The **BCP** does not cover third party resilience; however, subcontractors should be asked to provide evidence that they have considered potential resilience issues. Project offices are also encouraged to apply the principles of **BCM**.
2. The Business Continuity Plan (**BCP**) must include all-hazads, including the following main scenarios that can affect the continuity of operations:
3. Events resulting in incapacitation or loss of staff;
4. Events interrupting mission-critical systems;
5. Events resulting in loss of access to or loss of office building;
6. Events resulting in loss of vendors’ services.
7. The BCP follows International Best practices, ISO 22301 (Societal Security – Guidelines for Incident Preparedness and Operations Continuity Management).
8. Business Continuity Focal Points coordinate the preparation of BCPs for their offices/units. The **BCP** includes the following:
9. The List of all critical business functions with the names of staff supporting/performing those functions, including those that are outsourced, with a pre-determined time, procedures for business recovery,
10. The list of equipment and material required to carry out these functions,
11. The plan to communicate with internal and external partners,
12. The plan to set up alternate site when considered necessary.
13. It establishes clear management procedures, succession, delegation of authority, outlines arrangements for training, testing and maintenance.
14. The draft Business Continuity Plan (**BCP**) is submitted to **BMS** business continuity management focal point for technical review. Once reviewed, the BCP focal point finalizes the draft for Head of office’s approval.
15. Heads of offices/units must approve and sign the **BCP**. In addition, in order to be considered compliant with this policy and guideline, they should set clear testing and reviewing schedules for **BCP** (at least once a year or following an important change in BCP components). Testing and reviewing covers the following items:

a. Purpose and scope of the testing, simulation events for testing;

b. Time for the entire testing; staff evacuation procedures;

c. Emergency communication plans, critical data backup and retrieval;

d. Readiness of building/facilities and resources needed for testing;

e. Readiness of an alternative site for operations within specific timeframe;

f. Recovery of critical business functions.

Testing results will be evaluated and used to improve the BCP where necessary.

# Roles and Responsibilities for BCM

UNDP Bureau for Management Services (BMS)

1. Within the context of overall organizational risk management, BMS is responsible for the formulation and review of the corporate BCM Policy and its operationalization.
2. **BMS Directorate** provides technical support to Business Continuity Focal Points for the preparation of BIAs and BCPs, and keeps records of country offices/bureau/unit BCPs at the BCM SharePoint platform. BMS monitors country offices/bureau/units’ compliance and regularly updates the SMG on the status of BCM activities and offices’ compliance. BMS works closely with **Regional Bureaus (RBx)** and centers to ensure policy adherence of country offices and business units.
3. **Office of Information Technology (OIMT)** provides the necessary support (if needed) to Country Office’s Information Technology (IT) staff for the preparation of Information Technology Disaster Recovery (ITDR) Plans.

UNDP Security Management Group

1. Oversight of **BCM** activities is delegated to the Security Management Group. Business Continuity Management Plans are standing items on the SMG agenda at regular intervals.

Regional/Central Bureaus and Liaison offices:

1. Regional/Central Bureaus as well as Liaison offices oversees their respective regions and offices to ensure that Business Continuity Plans (**BCPs**) are updated and tested annually.

Heads of Country Offices, Bureau and Units

1. BCM activities should be included in CO/Bureau/unit work plans. A reference to the Business Continuity Management (**BCM**) responsibilities should be included in job descriptions to ensure that staff are aware of their personal role and responsibilities should a disruption occur.
2. Business Continuity Focal Points must be assigned to coordinate Business Impact Analysis (**BIA**) as well as the preparation and maintenance of Business Continuity Plans. The Business Continuity Focal Points work closely with staff covering the various functions including Senior Management as well as IT staff who are usually assigned to maintain **ITDR** Plans.

Line Managers

1. Managers at all levels should address business continuity regularly in team meetings and ensure that Business Continuity Management is part of the induction process for all new staff.

# Trigger for the activation of Business Continuity Plans

Headquarters (New York):

1. During incidents affecting all UNDP Operations in NY, the Security Management Group (**SMG**) will advise bureaus and units to activate their Business Continuity Plans (**BCPs**). In the case of incidents impacting only a particular unit/bureau (for example, limited fire), the director of the affected unit/bureau will activate its **BCP** and advise staff how to proceed based on the **BCP** of the unit).

Country Offices:

1. The Resident Representative will activate the Business Continuity Plan (**BCP**) based on the advice of the country **Security Management Team (SMT**).
2. To assure that the business continuity planning process is robustly driven, offices and units are required to use established internal resources. In addition, a **BCM** Management Specialist in Bureau of Management Services (**BMS**) has been assigned to help facilitate the overall coordination of **BCM**.

# Training, Exercising and Review

1. All BCPs are to be reviewed by **BCP** Focal Points at least annually or more regularly under the following conditions:
2. Updating contact information;
3. Following a change in the structure of the organization and/or office;
4. Following a change in staffing including critical staff;
5. In response to a signification new threat and risk assessment;
6. Changes in the national regulatory requirement.
7. The **BCP** must be exercised at least once every year. The format of the exercise may vary and advice can be provided by the Bureau of Management Services in coordination with Regional Bureaus and country offices.
* **Templates and Additional Resources:**
1. [Business Continuity Management User guide](https://popp.undp.org/node/4076/)
2. [English BCP Template and annexes – Country Offices](https://undp.sharepoint.com/teams/BCM/Shared%20Documents/Forms/AllItems.aspx?id=%2Fteams%2FBCM%2FShared%20Documents%2FCountry%20Offices%20BCP%20Related%20Templates%2FEnglish&viewid=4447ae9d%2D6e70%2D419c%2Db305%2D7601e8ba5baa)**\*[[1]](#footnote-1)**
3. [English BCP Template and annexes – HQ](https://undp.sharepoint.com/teams/BCM/Shared%20Documents/Forms/AllItems.aspx?id=%2Fteams%2FBCM%2FShared%20Documents%2FHQ%20BCP%20Related%20Templates&viewid=4447ae9d%2D6e70%2D419c%2Db305%2D7601e8ba5baa)
1. **\*Note**: Templates are also available in French and Spanish

 ([Business Continuity Management - Country Offices BCP Related Templates - All Documents (sharepoint.com)](https://undp.sharepoint.com/teams/BCM/Shared%20Documents/Forms/AllItems.aspx?id=%2Fteams%2FBCM%2FShared%20Documents%2FCountry%20Offices%20BCP%20Related%20Templates&viewid=4447ae9d%2D6e70%2D419c%2Db305%2D7601e8ba5baa) [↑](#footnote-ref-1)