United Nations Population Fund

**Delivering a world where every pregnancy is wanted,
every childbirth is safe and
every young person's potential is fulfilled**

OFFICE OF AUDIT AND INVESTIGATION SERVICES

AUDIT OF

BUSINESS CONTINUITY MANAGEMENT

IN UNFPA

FINAL REPORT
No IA/2024-23

20 December 2024

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Background

1.   The UNFPA Office of Audit and Investigation Services (OAIS) conducted an audit of Business Continuity Management (BCM) in UNFPA (the BCM process). The audit was undertaken from 24 April to 20 July 2024.

2.   BCM is a comprehensive process that ensures continuous operation of an organization by identifying potential threats, analysing their impact on business operations, and developing plans to mitigate disruption. The UNFPA BCM process is coordinated and managed by the Office of Security Coordinator (the Office).

3.   The overall objective of the audit was to review:

   a)   UNFPA's business continuity governance, policies, practices, plans, and testing procedures for completeness and alignment with the United Nations-wide Policy on the Organizational Resilience Management System (UN ORMS);[1] and
   b)   UNFPA's disruption readiness.

4.   To achieve the audit objective, three key areas of the BCM process were reviewed, namely:

   a)   Governance – Roles, responsibilities, policies, procedures, monitoring and oversight mechanisms, resources, and integration of BCM activities with other organizational processes;
   b)   Risk management – Risk management, business recovery strategies, and development of contingency plans to sustain critical functions during disruptive events; and
   c)   Readiness of contingency plans[2] and general awareness among personnel of their existence - Operation, maintenance, and review of contingency plans, training, awareness programmes, and testing exercises.

5.   The audit covered BCM activities undertaken from 1 January 2022 to 30 June 2023. The audit procedures undertaken were limited to reviewing and analysing, on a test basis, processes embedded in applicable policy,[3] and excluded the organization's security plan.

Methodology and scope

6.   The audit was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing of the Institute of Internal Auditors (The IIA).

7.   The audit methodology encompassed document review, interviews, and discussions with a broad range of stakeholders in UNFPA, spanning various seniority levels and geographical locations, including Headquarters and all six operational regions.[4] The audit applied International Standards (ISO 22301)[5] and the Policy on UN ORMS[1] as reference points in examining UNFPA policies and practices and benchmarking against other United Nations agencies. Additionally, a survey was conducted to obtain feedback from

---

[1] UN ORMS is a comprehensive emergency management system, linking various actors and activities across preparedness, prevention, response, and recovery, to enhance the Organization's resilience and capacity to effectively manage the risks of disruptive events.

[2] Contingency plans include: (a) business continuity plans set into context with office-specific risks of disruptions to the applicable security risk management process that align to the United Nations Country Team (UNCT) response for UNFPA mandate-related aspects; and (b) disaster recovery plans that capture, in single repositories, all information that describes the ability of UNFPA Country Offices to withstand disasters and the processes that must be followed to achieve disaster recovery.

[3] Policy and Procedures for Business Continuity Management, March 2023.

[4] Asia Pacific, Eastern Europe and Central Asia, East and Southern Africa, Latin America & the Caribbean, and West and Central Africa.

[5] ISO 22301:2019 is the international standard that specifies requirements for establishing, implementing, maintaining, and continually improving a Business Continuity Management System.

business continuity focal points stationed at UNFPA field offices. The survey focused on key aspects of the BCM process such as policy implementation, risk management, training, communication protocols, and lessons learned from previous incidents.

Overall audit rating

8.		The overall audit rating is "***Partially Satisfactory with Some Improvement Needed***",[6] which means that the assessed governance arrangements, risk management practices, and controls were adequately designed and operating effectively but needed some improvement to provide reasonable assurance that the objectives of the audited entity/area should be achieved. The issues and improvement opportunities identified did not significantly affect the achievement of the audited entity/area objectives. Management action is recommended to ensure that identified risks are adequately mitigated.

9.		The audit provided recommendations to address the following issues: (a) outdated Business Continuity Management policies, procedures and guidance; (b) inadequate risk assessment in the development of Business Continuity Plans; (c) inadequate disruption impact analysis and recovery planning; and (d) noncompliance with requirements for updating and testing Business Continuity Plans.

10.		Ratings by key audit area are summarized in the following table.

Audit ratings by key audit area		
Governance		**Some improvement needed**
Risk Management		**Some improvement needed**
Readiness of Contingency Plans		**Some improvement needed**

Good practice identified

11.		There was an established crisis response mechanism in place, activated through a Crisis Response Team at UNFPA Headquarters that comprises key persons to manage corporate responses to critical incidents or crises affecting UNFPA in its field offices.[7]

Key recommendations Total = **5**, High priority = **0**

12.		No high-priority recommendation was identified. All five recommendations issued were of medium priority.

13.		The audit provided recommendations to address the following issues: (a) outdated Business Continuity Management policies, procedures and guidance; (b) inadequate risk assessment in the development of Business Continuity Plans; (c) inadequate disruption impact analysis and recovery planning; and (d) noncompliance with requirements for updating and testing Business Continuity Plans.

Implementation status of previous OAIS recommendations

14.		The BCM process has not previously been audited by OAIS. The United Nations Board of Auditors audited the UNFPA Business Continuity Plan (BCP) in 2022. The only recommendation arising from the 2022 audit was fully implemented and closed.

---

[6] See complete set of definitions in Annex 1.

[7] Field offices include Country, Regional, Sub-Regional, and Liaison Offices.

Management comments and action plan

15.   Office Management accepts all the recommendations provided in this report and welcomes the in-depth review of the BCM process. The areas identified for improvement will be implemented in accordance with the operational plan, as specified in the responses to each of the recommendations.

16.   The OAIS team wishes to thank Management and personnel of the Office of Security Coordinator, Information Technology Solutions Office, and various Headquarter units and field offices for their cooperation and assistance throughout the audit.

Signed by:

Moncef Ghrib

50458A3AFD0C4EF...

Moncef Ghrib
Director
Office of Audit and Investigation Services

I.   AUDIT BACKGROUND

1.   BCM is a comprehensive process that ensures continuous operation of an organization by identifying potential threats, analyzing their impact on business operations, and developing plans to mitigate disruption. It is an integral part of UNFPA's governance framework and part of the Organization's Enterprise Risk Management (ERM). Therefore, embedded in various management processes, including, but not limited to, security, finance, reputational and programme risk management. The BCM process is also harmonized with other organizational preparedness efforts[8] such as emergency response and crisis management plans.

2.   There is shared responsibility for the BCM process across all UNFPA offices, with each office tasked with its implementation and maintenance. UNFPA's BCM policy[3] provides a framework for assisting UNFPA business units to continue critical functions in the event of a direct or indirect crisis affecting implementation of the Organization's mandate. Owners of business-critical services are required to ensure that contingency plans[2] are developed, maintained, and tested to maintain service continuity during high-impact incidents.[9]

3.   Each business unit's Business Continuity Plan (BCP) implements the BCM policy by turning strategic goals into practical actions to ensure organizational resilience, personnel safety, and continuity of critical functions during disruption. Aligned with the BCM policy, BCPs provide operational frameworks for risk identification, incident response, and recovery strategies, ensuring that UNFPA can quickly restore operations. The key elements of a BCP include:

   a) Risk assessment - continuously evaluating risks to critical functions;
   b) Crisis management - coordinated response for rapid decision-making and communication;
   c) Recovery planning - detailed steps to restore essential services;
   d) Personnel safety - prioritizing staff security while ensuring crisis leadership; and
   e) Scenario-based testing - regular exercises to enhance preparedness.

4.   The Office of Security Coordinator (OSC) is responsible for providing guidance, support, and oversight in implementing the BCM process. It regularly reports to UNFPA senior management on progress made. The Information Technology Solutions Office (ITSO) is tasked with ensuring continuity and recovery of critical Information and Communication Technology (ICT) systems. Heads of Offices[10] are required to provide BCM progress updates to OSC, manage BCM responses during disruptions, and establish a Crisis Response Team (CRT).[11] In addition, training of personnel responsible for BCP-related functions plays a critical role in the successful implementation of BCPs.

5.   As set out in the 2024 OAIS Annual Work Plan, an audit of the UNFPA Business Continuity Management process was conducted in conformance with the International Standards for the Professional Practice of Internal Auditing (promulgated by the IIA), which requires that internal auditors plan and perform the audit to obtain reasonable assurance on the adequacy and effectiveness of the governance, risk management, and internal control processes in place. The overall objective of the audit was to review:

   a) UNFPA's business continuity governance, policies, practices, plans, and testing procedures for completeness and alignment with the United Nations-wide Policy on the Organizational Resilience Management System (UN ORMS); and
   b) UNFPA's disruption readiness.

---

[8] Policy and Procedures for Business Continuity Management, March 2023.

[9] The UNFPA Information Security Policy, January 2023 (revised January 2024).

[10] Directors, Representatives, and Heads of Field Offices.

11 The Crisis Response Team comprises UNFPA personnel responsible for time-critical activities and is chaired by the Representative at the country office level.

6.   To achieve the audit objective, three key areas of the BCM process were reviewed, namely:

   d)   Governance – Roles, responsibilities, policies, procedures, monitoring and oversight mechanisms, resources, and integration of BCM activities with other organizational processes;

   e)   Risk management – Risk management, business recovery strategies, and development of contingency plans to sustain critical functions during disruptive events; and

   f)   Readiness of contingency plans[2] and general awareness among personnel of their existence - Operation, maintenance, and review of contingency plans, training, awareness programmes, and testing exercises.

7.   The audit adopted a risk-based approach, with audit tests focusing on high- and medium-risk processes. The audit procedures undertaken were limited to reviewing and analyzing, on a test basis, processes embedded in applicable policy,[3] and excluded the organization's security plan.

8.   The audit methodology encompassed document review, interviews, and discussions with a broad range of stakeholders in UNFPA, spanning various seniority levels and geographical locations, including Headquarters and all six operational regions. The audit applied International Standards (ISO 22301)[5] and the Policy on UN ORMS[1] as reference points in examining UNFPA policies and practices and benchmarking against other United Nations agencies. Additionally, a survey was conducted to obtain feedback from business continuity focal points stationed at UNFPA field offices. The survey focused on key aspects of the BCM process such as policy implementation, risk management, training, communication protocols, and lessons learned from previous incidents. Out of 70 offices surveyed, 40 (57 per cent) responded.

II.   AUDIT RESULTS

9.   The audit results are presented below, by audit area.

A. GOVERNANCE	SOME IMPROVEMENT NEEDED

10.   There was an established crisis response mechanism in place, activated through a Crisis Response Team at UNFPA Headquarters that comprises key persons to manage corporate responses to critical incidents or crises affecting UNFPA in its field offices.[7]

11.   The following matters that require management attention were noted.

Issue 1   Insufficient personnel and technological resources dedicated to BCM activities

12.   Standards[12] prescribe strong BCM governance, requiring leadership commitment, clear roles and responsibilities, adequate resources, and regular reviews to ensure organizational resilience. The following challenges in implementing and maintaining BCM practices were identified, mainly due to significant resource constraints in personnel and information technology.

a) *Personnel dedicated to BCM activities* - Of 20 approved posts in OSC, 9 (45 per cent) were vacant. At the time of the audit fieldwork, a reorganization of OSC human resources and its organizational structure was underway to incorporate dedicated personnel to coordinate BCP activities in the Organization. Hiring processes for the vacant posts, which included upgrading five regional and headquarter positions and creating national officer posts in four regions to serve as deputies to regional security advisers, were expected to be completed by the end of the fourth quarter of 2024. The new structure aims to address service delivery and advisory gaps related to the BCM process and staff safety and security. Prior to the reorganization, OSC had not received additional budgetary support since taking on its BCM responsibilities back in 2017, posing increased workload challenges.

b) *Information Technology Integration* - BCM activities did not fully employ the technology available within UNFPA. While a centralized repository for contingency plans was in place, manual data collection, incident logging, post-crisis analysis, and reporting caused significant inefficiencies. Stakeholders interviewed highlighted limited use of data analytics tools to identify trends and risks, hindering proactive risk management. There was evidence of discussions between OSC and ITSO regarding the potential use of Quantum[13] for effective execution of BCM activities and development of a customized dashboard to integrate key BCM performance metrics. Office Management stated that BCM roles and responsibilities are clearly defined in corporate policies and procedures and that automating time-consuming manual processes would simplify BCP implementation, monitoring, and oversight.

ROOT CAUSE   *Resources: insufficient resources (financial, human, and technical).*

IMPACT   *There is increased vulnerability to disruptions, potentially delaying recovery efforts and compromising operational continuity.*

CATEGORY   *Strategic.*

---

[12] ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements, and UN ORMS, as set forth in CEB/2014/HLCM/17.
[13] UNFPA's Enterprise Resource Planning system.

> **OAIS comment:**
>
> Given the proactive steps already taken by Office Management, including undertaking a human resources realignment exercise, creating a dedicated BCM position, as well as the ongoing effort to explore relevant IT solutions to streamline the BCM process, no recommendation is issued in this regard. While acknowledging the progress made, the importance of ensuring that these measures are fully implemented in a timely manner is hereby emphasized.

Issue 2   Outdated policies, procedures and guidance

13.   Five out of nine BCM-related policies and guidance notes included in the UNFPA Policies and Procedures Manual (PPM) were outdated. A critical document[14] (one of the five) that outlines corporate response protocols for managing critical incidents and identifies the key personnel responsible for crisis management was outdated. At the time of finalizing this report, Office Management had prepared a revised version of the document that was still in draft form.

14.   Although not formally part of the PPM, guidance notes[15] are accessible through it. Four guidance notes[16] reviewed required updating. Office Management indicated that the documents were obsolete as most of their contents were integrated into a UNFPA Crisis Management Handbook. Consequently, Management formally requested their removal from the PPM.

15.   At the time of finalizing this report, only two important documents required minor revisions.[17] Further, while established guidelines for ICT disaster recovery were in place, a policy on disaster recovery or other comprehensive guidance were yet to be finalized and approved. Such policy or guidance are crucial as they would establish a structured framework for disaster recovery planning and guide implementation of ICT disaster recovery processes. It would also clearly define the roles, responsibilities, and reporting structures for disaster recovery planning, testing, and compliance monitoring, ensuring consistent and accountable disaster recovery efforts across all UNFPA offices.

ROOT CAUSE	*Guidelines: inadequate corporate policies, procedures, and guidance.*
IMPACT	*The Organization's ability to effectively manage critical incidents and disaster recovery is diminished, increasing the risk of operational disruptions, delayed responses, and noncompliance with applicable standards.*
CATEGORY	*Operational.*

Recommendation 1	**Priority: Medium**
Update and finalize the relevant Business Continuity Management related policy and guidance documents in the Policies and Procedures Manual, particularly the critical Standard Operating Procedures (SOP) for Management of a Critical Incident by the Headquarters Crisis Response Team and other related procedures for field offices.	

---

[14] Standard Operating Procedures for Management of a Critical Incident by Headquarters Crisis Response Team (CRT), October 2017.

[15] Tools, guidance notes and strategy documents are issued outside of the PPM and contain relevant and useful information for programming and management activities.

[16] Guidance Note on Office Relocation (2016), Guidelines for Security Focal Points (2011), Safety & Security - FAQ (2015), and Worksheet for Assessing MOSS & Premises Security funding needs (2016).

[17] Standard Operating Procedures for Management of a Critical Incident by Headquarters Crisis Response Team (CRT), October 2017, and Guidance Note on UNFPA Fire Safety (2014).

Manager Responsible for Implementation: Chief, OSC.
Status: *Agree.*
Management action plan:
A revised version of the CRT-SOP for Managing Safety and Security Critical Incidents is being reviewed in conjunction with the Secretariat of the UNFPA Programme Division. It incorporates proposed edits by OAIS and is expected to be finalized by the end of 2024.
Estimated completion date: *January 2025.*

Recommendation 2	Priority: Medium
Establish guidance on Information Technology disaster recovery to serve as a comprehensive framework for data and IT systems recovery. The guidance should include a clarification of roles, responsibilities, testing requirements, and timelines to support consistent and effective recovery actions across all UNFPA offices.	
Manager Responsible for Implementation: Director, ITSO.	
Status: *Agree.*	
Management action plan:	
Management will establish new guidelines for establishing and testing Information Technology Disaster Recovery Plans (DRP), commensurate with risk profiles for each location where an IT DRP is required.	
Estimated completion date: *July 2026.*	

B. RISK MANAGEMENT	**SOME IMPROVEMENT NEEDED**

Issue 3   Inadequate risk assessment in the development of Business Continuity Plans

16.   Policy[18] establishes that the BCM process is part of Organization's ERM, embedded in various management processes, including, but not limited to, security, finance, reputational and programme risk management. Further, the process is harmonized with other organizational preparedness efforts. A corporate BCP template[19] requires preparation, by UNFPA offices, BCPs tailored to office-specific risks of disruption and the applicable Security Risk Management (SRM)[20] process, including the security plan and contingency plans. The template allows for alignment with United Nations Country Team (UNCT) responses for UNFPA mandate-related aspects. Further, the template indicates that the key parameters for BC/ORMS[21] planning

---

[18] Policy and Procedures for Business Continuity Management, March 2023.

[19] UNFPA BCP template revised (28 March 2023).

[20] Security Risk Management (SRM) is the United Nations system-wide process to assess specific threat categories, such as Crime, Terrorism, Armed Conflict, Civil Unrest, and Hazards.

[21] BC/ORMS refers to the integration of Business Continuity (BC) planning with the UN ORMS. ORMS is an UN-wide framework for emergency management, and UNFPA's BC planning is designed to align with it.

are the anticipated risks of disruption(s). These disruption risks should be obtained from various risk assessments.[22]

17.   Risk management was not comprehensively integrated into the BCP development process. A review of 18 BCPs sampled for testing showed that most plans focused on operational and security threats,[23] with limited consideration of strategic risks such as funding cuts, reputational damage, and political risk. This indicates gaps in preparedness for a broader range of disruptions. Office Management acknowledged that the existing BCP template primarily focused on disruption scenarios such as armed conflict, civil unrest, terrorism, crime, and natural disasters - often with predefined mitigation measures (e.g., armored vehicles, protective gear, and specialized training).

18.   UNFPA staff interviewed[24] indicated inconsistencies across offices in the application of risk assessment principles, leading to variations in how risks were integrated into BCPs. For example, several offices relied heavily on historical security incidents, while others depended on the insights of individual BCP focal points and heads of office. Various offices expressed concern about overlapping risk assessments (i.e., ERM, SRM, Minimum Preparedness Actions,[25] and BCP), which create a duplication of effort and contribute to a sense of confusion, making it difficult to prioritize preparedness activities.

19.   Additionally, many offices depended solely on prefilled templates and generic disruption scenarios without considering the unique risks facing them. None of the 18 BCPs tested included disruption scenarios peculiar to the offices that prepared them, limiting their ability to address office-specific vulnerabilities to disruption.

ROOT CAUSE	*Guidelines: inadequate business continuity planning (inadequate risk management assessment)*
IMPACT	*BCPs may overlook critical risks not explicitly addressed in predefined scenarios, leaving the Organization vulnerable to disruptions.*
	Inadequate risk assessments in the BCP development process undermine the Organization's ability to effectively respond to disruption incidents.
CATEGORY	*Operational.*

Recommendation 3	Priority: Medium
Train personnel who perform BCP-related functions, including Crisis Response Team members, to enhance their knowledge and understanding of preparing, validating, and implementing Business Continuity Plans, as well as developing and validating local risk scenarios for inclusion in risk assessments.	
Manager Responsible for Implementation: Chief, OSC, in collaboration with the UNFPA Chief Risk Officer.	
Status: *Agree.*	

---

[22] ERM, SRM, and humanitarian and disaster risk assessments.

[23] Security threats such as Crime, Terrorism, Armed Conflict, Civil unrest, and Hazards.

[24] Business Continuity Focal Points, Humanitarian Advisors, and Regional Security Officers.

[25] Minimum Preparedness Actions define a set of actions that strengthen a country's ability to respond to emergencies.

Management action plan:
This need was identified through OSC monitoring of BCP implementation. To enhance the knowledge and understanding of personnel performing BCP-related functions, OSC will standardize the training package specifically designed for this purpose, improving the integration programmatic and risk assessment aspects. To implement these activities, OSC has included in the 2025-2028 corporate resources funding for the development of training materials.
Estimated completion date: *December 2026.*

Issue 4.   Inadequate disruption impact analysis and recovery planning

20.   Policy requires the inclusion, in BCPs, of an analysis of time-critical activities and functions based on Disruption Impact Analysis (DIA). The BCP template requires the CRT to analyze disruption risk and its impact, forming the basis for identifying time-critical activities and functions (TCAF).[26]

21.   Review of the 18 BCPs and interviews with 8 Country Offices identified the following gaps:

a) *Limited evidence of DIA*: Eight BCPs lacked documentation to demonstrate how disruption risks and functions were assessed, raising concern about the thoroughness of their preparation. Further, there was no formal methodology for completing DIA and identifying critical business risks. Staff interviewed revealed inconsistencies in their understanding and conduct of DIA. Some relied heavily on predefined TCAFs outlined in the BCP template, while others were unaware that DIA was necessary beyond predefined scenarios in the template;

b) *Inadequate consideration of interdependencies:* Offices did not adequately identify and map critical interdependencies and consider how different parts of the Organization would be affected during a disruption. For instance, one BCP reviewed focused on restoring physical workspace following a natural disaster but failed to consider other risks such as supply chain disruptions that could impact the delivery of UNFPA's mandate;

c) *No recovery time objectives:* The BCPs did not define Recovery Time Objectives (RTO). RTOs are critical for prioritizing recovery actions. DIA informs the determination of RTOs, which in turn guide the development of recovery strategies. This is essential to determining the maximum tolerable downtime for each system or process during a disruption. Without RTOs, offices may face challenges in effectively prioritizing and allocating resources during disruptions; and

d) *Lack of data-driven disruption duration estimates:* Most BCPs used generic estimates or did not indicate any (i.e., left blank) for disruption duration,[27] without supporting data – suggesting lack of thorough analyses regarding the potential impact of disruptions. Four out of the 18 BCPs (22 per cent) did not specify duration estimates for potential disruptions, while the rest used broad or generic estimates without documented justification or supporting data.

---

[26] Time-critical business services include pre-identified critical processes/functions as outlined in respective offices' BCP.

[27] Predictions or estimates of how long a disruption (e.g., natural disaster, cyberattack) is likely to last.

ROOT CAUSE	*Guidelines: inadequate planning and corporate guidelines (lack of a formalized and standardized methodology for conducting DIA).*
IMPACT	*Offices may fail to fully appreciate how disruption impacts services, the services to prioritize during a disruption, and prioritization of resources in such a scenario.*
CATEGORY	*Operational.*

Recommendation 4	**Priority: Medium**
Leveraging the ongoing corporate-level technology integration initiatives, establish a standardized, automated process to document, track, and report on business continuity planning activities, in alignment with policy requirements. The process should include the development of Disruption Impact Analysis and recovery planning, incorporate tools to standardize and automate all business continuity planning phases (i.e., development, validation, implementation, and testing), and provide accessible, real-time data for ongoing compliance and performance monitoring across all UNFPA offices.	
Manager Responsible for Implementation: Chief, OSC, in collaboration with the Director, ITSO.	
Status: *Agree.*	
Management action plan: As part of a phased approach toward a fully integrated Business Continuity Management framework within Quantum Plus, the Office has initiated the recommended efforts and is collaborating with ITSO. Office Management held a series of meetings and consultations in 2024 with the Programme Division Dashboard Team and ITSO. The required process and automation are scheduled to be completed in 2026 and will be integrated into corporate Quantum Plus initiatives.	
Estimated completion date: *December 2026.*	

C. READINESS OF CONTINGENCY PLANS	**SOME IMPROVEMENT NEEDED**

Issue 5   Noncompliance with BCP update and testing requirements

22.   Policy requires the local CRT to review and validate the BCP annually and to update it after each activation. Similarly, the ICT Disaster Recovery Guidelines for UNFPA Offices require updating of DRPs within three months of changes to disaster recovery arrangements, ICT systems, infrastructure, or key personnel. Both plans (collectively known as contingency plans) should be regularly updated to ensure accuracy of contact information, appropriate team structures, and alignment with evolving office needs.

23.   Update and review of contingency plans:

a) *BCPs:* As of June 2024, 42 out of 136 (31 per cent) BCPs were yet to be reviewed or updated within the required time limit. Some plans contained outdated contact information, posing a risk to effective crisis management; and

b) *DRPs:* Eight out of 18 (44 per cent) of DRPs tested were yet to be reviewed or updated to reflect staff changes and revisions that went beyond the three-month ICT disaster recovery guideline. The repository also contained earlier or outdated DRP versions that had already been revised and updated by offices.

24.   Moreover, in accordance with policy, yearly exercises to validate BCP scenarios are to be conducted based on prevailing circumstances at each duty station or office to ensure their effectiveness and identify areas for improvement. The BCP template requires that offices document the date, activities undertaken, and lessons learned from any business continuity exercises or actual events. Similarly, the ICT Disaster Recovery Guidelines for UNFPA Offices prescribe periodic tests to enhance and verify disaster recovery arrangements for critical ICT systems. In 2023, ITSO issued a directive via an official memorandum mandating all UNFPA offices to formally document their DRPs and submit test results by the end of the second quarter of 2024.

25.   Testing and validation of contingency plans:

   a) A review of BCPs in the central depository revealed that offices did not document the testing of their respective BCPs Testing rates ranged from zero to 79 per cent, with several BCPs developed but not tested. Three of the eight offices tested did not provide evidence of BCP testing; and

   b) The DRP central repository, which contained only the 2023 DRPs (as per the annual uploading requirements) at the time of the audit fieldwork, showed disparities between completion rates for DRP development and their testing. Explanations provided by ITSO indicated that it initiated a structured approach to disaster recovery planning and testing in 2023, with the aim of developing DRPs testing them in 2024. As of August 2024, 40 out of 128 offices (31 percent) had completed and documented their DRP tests.

ROOT CAUSE   *Guidance: inadequate supervision at the Office and Headquarters level (contingency plans not regularly reviewed, updated, or tested).*

IMPACT   *Failure to regularly update and test contingency plans undermines the Organization's ability to manage disruptions, raising serious concerns about its preparedness for operational continuity in such eventualities.*

CATEGORY   *Compliance.*

Recommendation 5	**Priority: Medium**
Raise staff awareness of the importance of regularly updating and testing contingency plans. Additionally, implement monitoring and reporting controls to improve compliance with policy requirements regarding: (a) updating of contingency plans; and (b) scheduling of contingency plan tests.	
Manager Responsible for Implementation: Chief, OSC, and the Director, ITSO.	
Status: *Agree.*	
Management action plan: The recommended activities will be integrated as part of the OSC annual plan and serve as mandatory tasks for UNFPA offices. Dedicated outputs and activities will be included in the corporate planning tool (Quantum Plus).	
Estimated completion date: *December 2025.*	

ANNEX I - DEFINITION OF AUDIT TERMS

A. AUDIT RATINGS

Audit rating definitions, adopted for use in reports for audit engagements initiated as from 1 January 2016,[28] are explained below:

▪ **Satisfactory**	🟩	The assessed governance arrangements, risk management practices and controls were adequately designed and operating effectively to provide reasonable assurance that the objectives of the audited entity/area should be achieved. The issue(s) and improvement opportunities identified, if any, did not affect the achievement of the audited entity or area's objectives.
▪ **Partially satisfactory with some improvement needed**	🟨	The assessed governance arrangements, risk management practices and controls were adequately designed and operating effectively but needed some improvement to provide reasonable assurance that the objectives of the audited entity/area should be achieved. The issue(s) and improvement opportunities identified did not significantly affect the achievement of the audited entity/area objectives. Management action is recommended to ensure that identified risks are adequately mitigated.
▪ **Partially satisfactory with major improvement needed**	🟧	The assessed governance arrangements, risk management practices and controls were generally established and functioning but need major improvement to provide reasonable assurance that the objectives of the audited entity/area should be achieved. The issues identified could significantly affect the achievement of the objectives of the audited entity/area. Prompt management action is required to ensure that identified risks are adequately mitigated.
▪ **Unsatisfactory**	🟥	The assessed governance arrangements, risk management practices and controls were not adequately established or functioning to provide reasonable assurance that the objectives of the audited entity/area should be achieved. The issues identified could seriously compromise the achievement of the audited entity or area's objectives. Urgent management action is required to ensure that the identified risks are adequately mitigated.

B. CATEGORIES OF ROOT CAUSES AND AUDIT ISSUES

Guidelines: absence of written procedures to guide staff in performing their functions
- Lack of or inadequate corporate policies or procedures
- Lack of or inadequate Regional and/or Country Office policies or procedures
- Inadequate planning
- Inadequate risk management processes
- Inadequate management structure

Guidance: inadequate or lack of supervision by supervisors
- Lack of or inadequate guidance or supervision at the Headquarters and/or Regional and Country Office level
- Inadequate oversight by Headquarters

Resources: insufficient resources (funds, skills, staff) to carry out an activity or function:
- Lack of or insufficient resources: financial, human, or technical resources

---

[28] Based on the proposal of the Working Group on harmonization of engagement-level audit ratings approved by the United Nations Representatives of Internal Audit Services (UN-RIAS) in September 2016.

▪ Inadequate training

Human error: un-intentional mistakes committed by staff entrusted to perform assigned functions

Intentional: intentional overriding of internal controls.

Other: factors beyond the control of UNFPA.

C. PRIORITIES OF AGREED MANAGEMENT ACTIONS

Agreed management actions are categorized according to their priority, as a further guide to Management in addressing the related issues in a timely manner. The following priority categories are used:

▪ **High**   Prompt action is considered imperative to ensure that UNFPA is not exposed to high risks (that is, where failure to take action could result in critical or major consequences for the organization).

▪ **Medium**   Action is considered necessary to avoid exposure to significant risks (that is, where failure to take action could result in significant consequences).

▪ **Low**   Action is desirable and should result in enhanced control or better value for money. Low priority management actions, if any, are discussed by the audit team directly with the Management of the audited entity during the course of the audit or through a separate memorandum upon issued upon completion of fieldwork, and not included in the audit report.

D. CATEGORIES OF ACHIEVEMENT OF OBJECTIVES

These categories are based on the COSO framework and derived from the INTOSAI GOV-9100 Guide for Internal Control Framework in the Public Sector and INTOSAI GOV-9130 ERM in the Public Sector.

▪ **Strategic**   High level goals, aligned with and supporting the entity's mission

▪ **Operational**   Executing orderly, ethical, economical, efficient and effective operations and safeguarding resources against loss, misuse and damage

▪ **Reporting**   Reliability of reporting, including fulfilling accountability obligation

▪ **Compliance**   Compliance with prescribed UNFPA regulations, rules and procedures, including acting in accordance with Government Body decisions, as well as agreement specific provisions

GLOSSARY

Acronym	Description
BCM	Business Continuity Management
BCP	Business Continuity Plan
CRT	Crisis Response Team
DIA	Disruption Impact Analysis
DRP	Disaster Recovery Plan
ERM	Enterprise Risk Management
ERP	Enterprise resource planning
FAQ	Frequently Asked Questions
ICT	Information and Communication Technology
IIA	Institute of Internal Auditors
ISO	International Organization for Standardization
ITSO	Information Technology Solutions Office
OAIS	Office of Audit and Investigation Services
OSC	Office of Security Coordinator
PPM	Policies and Procedures Manual
RTO	Recovery Time Objective
SOP	Standard Operating Procedure
SRM	Security Risk Management
TCAF	Time-critical activities and functions
UN	United Nation
UNCT	United Nations Country Team
UN ORMS	United Nations Organizational Resilience Management System
UNFPA	United Nations Population Fund