SAVING
LIVES
CHANGING
LIVES

Internal Audit of Business Continuity Management in WFP

Office of the Inspector General
Internal Audit Report AR/21/03

March 2021

WFP
World Food
Programme

Contents

Internal Audit of Business Continuity Management in WFP

I. Executive Summary

Objective and scope of the audit

1. As part of its annual work plan, the Office of Internal Audit conducted an audit of WFP's Business Continuity Management. Special consideration was given to the impact of the COVID-19 pandemic and the remote working arrangements. Business Continuity Management is defined as "*a process that strengthens the ability of WFP to plan for and respond to potential threats, and to maintain the continuity of its critical business processes at a minimum agreed level following disruptive events*".[1]

2. The United Nations Organizational Resilience Management System,[2] the emergency management framework for the United Nations system, is an integral element of WFP's Business Continuity Management, providing an integrated framework for building and maintaining WFP's organizational resilience. Business Continuity Management includes measures to reduce WFP's vulnerability and improve the organization's capacity to manage crises and critical incidents.

3. The audit applied ISO 22301:2019 security and resilience – Business Continuity Management systems – as a reference standard to examine WFP's policies and practices. ISO 22301:2019 was also used to provide advice based on internationally recognized standards and best Business Continuity Management practices. A sample of six headquarters units and divisions, six Regional Bureaus and eight Country Offices were selected to assess the adequacy, efficiency and effectiveness of Business Continuity Management throughout WFP.

4. The audit focused on the period from 1 January to 31 August 2020. The audit team conducted the fieldwork for this audit from 12 October to 13 November 2020 at WFP headquarters in Rome with external consultants' assistance. The audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*.

Audit conclusions and key results

5. Based on the results of the audit, the Office of Internal Audit has come to an overall conclusion of **partially satisfactory / some improvement needed**. The assessed governance arrangements, risk management and controls were generally established and functioning well but needed improvement to provide reasonable assurance that the objective of the audited entity/area should be achieved. Issues identified by the audit were unlikely to significantly affect the achievement of the objectives of the audited entity/area. Management action is recommended to ensure that identified risks are adequately mitigated.

6. WFP's existing risk management practices effectively contribute to organizational resilience. As an organization that continuously responds to global emergencies, WFP is, to some extent, resilient by nature. However, some of WFP's Business Continuity Management objectives have yet to be fully addressed as described below.

7. A corporate Crisis Management Team was established at the onset of the COVID-19 pandemic to direct and oversee the organization's response, activating WFP's Business Continuity Plan. The Office of Internal Audit

[1] Executive Director's Circular, WFP Business Continuity Management, Circular No. OED2016/012.

[2] Policy on the Organizational Resilience Management System, Chief Executives Board, UN, effective 1 December 2014, which identifies the following key elements: (a) crisis management decisions making and operations coordination, (b) security support and response, (c) crisis communications, (d) mass casualty incident response, (e) IT disaster recovery, (f) business continuity, and (g) support to staff, survivors and their families.

observed that all sampled Regional Bureaus and Country Offices promptly appointed a Crisis Management Team (or equivalent) to direct and oversee their local response. Countries that already had Business Continuity Plans were required to adjust or update them, with most offices performing remote working simulations before the outbreak of COVID-19 in their countries. These exercises' lessons helped WFP address emerging issues and ensured employees' full remote-working capabilities continued uninterrupted. This is also thanks to the slow onset of the COVID-19 pandemic allowing time for WFP to think through its response from a corporate perspective. In addition, WFP headquarters promptly coordinated guidelines for COVID-19 response, which Regional Bureaus and Country Offices contextualized and complemented to manage the continuity of their operations during the pandemic.

8. WFP's investment in digitization and the adoption of cloud-based computing helped increase systems' resilience and capacity to respond to the rapid scale-up of remote connections and access to critical systems and data. During the audit period, there was a marked increase in the number of requests for IT support; the IT Service Helpdesk successfully managed these with existing resources thanks to the automation of IT users access requests. The Technology division's attention to cyber security risk during the pandemic was noteworthy. At the time of the audit, over 20 Country Offices had included the risk of cyber-attacks in their risk registers, indicating an increasing level of awareness in the organization. The Office of Internal Audit further corroborated improvements in 23 of 30 cyber security capabilities in 2020 when compared to 2017.[3]

9. The structure for Business Continuity Management envisaged in the current policy was not in place. In practice, the Crisis Management Team was active throughout the period audited and assumed responsibility for Business Continuity Management. Yet the Team is not set up and structured to continuously evaluate, direct and monitor the efficiency, effectiveness and performance of Business Continuity Management. Staffing and resource gaps were the root cause of many of the observations in this report.

10. The ultimate responsibility for safeguarding and testing critical business processes lies with process owners. Due to its limited authority and resources, the Business Continuity Management Team could not adequately support, coordinate and oversee such testing, monitoring and performance evaluation for both the Business Continuity and Disaster Recovery Plans. Periodic reviews of the test results and any remedial actions were not monitored by management, indicating that Business Continuity Management mechanisms and resource allocation needed reassessing.

Actions agreed

11. The audit report contains three high and five medium priority observations. Various divisions and governance bodies are responsible for implementing these agreed actions in coordination with relevant business process owners. Management has agreed to address the reported observations and implement the agreed actions by their respective due dates.

12. The Office of Internal Audit would like to thank managers and staff for their assistance and cooperation during the audit.

Anita Hirsch
Acting Inspector General

[3] Cyber Security Assurance Advisory, Current State Assessment, Benchmarking and High-Level Map (AA-21-01).

II. Context and Scope

WFP context

13. To achieve its strategic objectives, WFP provides food assistance that protects the safety, dignity and integrity of the most vulnerable populations and those in desperate need. Such life-saving assistance requires continuous delivery; therefore, WFP must maintain comprehensive Business Continuity (BC) capabilities. BC establishes the uninterrupted support required to critical programmes and partners, while ensuring staff health and safety.

14. Business Continuity Management (BCM) must be embedded in WFP's corporate culture and integrated with other WFP preparedness and response activities, including elements of WFP's Organizational Resilience Management System (ORMS).

15. The ORMS, as stipulated by WFP's BCM policies, should be maintained at a state of readiness by the Organizational Resilience Management Group (ORMG), comprised of representatives from the organization's functional areas responsible for critical business processes. The ORMG supports the Crisis Management Team (CMT), chaired by the Deputy Executive Director (DED), who makes decisions on preparing and responding to critical incidents at headquarters and WFP crises.

Business Continuity Policies

16. Three circulars were approved in 2016, later referred to as BCM policies, to help WFP respond, recover, resume and restore operations in a crisis or critical incidents. These are:

- OED2016/010 - Organizational Resilience Management
- OED2016/011 - Crisis Management
- OED2016/012 - Business Continuity Management

17. BCM plans are mandatory at headquarters. Regional Bureaus (RBs) are responsible for maintaining preparedness of devolved critical business processes and incorporating BCM planning in the Emergency Preparedness and Response Package (EPRP) at the regional level. BCM policies extend to RBs and Country Offices (COs) as desirable objectives rather than mandatory policy requirements.

18. For field operations, BC is, to some extent, addressed through the implementation of the EPRP, and the support provided by RBs and WFP headquarters. An RB or CO may choose to prepare a BCP (RB/CO-BCP) and request support from the headquarters BCM Team. However, to effectively respond to the COVID-19 pandemic, BCPs were made mandatory for RBs and COs, underlining the usefulness of BCPs at all organization levels.

19. The Business Impact Analysis (BIA) performed in 2016 identified 56 business processes as critical, defining three impact scenarios to help WFP organize its BC response actions, as indicated below:

i. No access to premises – Work from home or work from alternative locations

ii. Devolution of critical business processes – Others elsewhere execute critical business processes

iii. No access to systems – Manual procedures are implemented to continue operations

20. The devolution model (ii) identifies the WFP offices that will take over 19 specific critical processes from headquarters in case of a disruptive incident. At the time of the audit, WFP had completed testing the devolution of payment and treasury processes and completed an exercise for payroll out of the 19 critical processes identified for devolution.

21. The periodic review of the BCM policies is necessary to adjust it to changing risks, operational context and technology advancements. The Executive Director Circulars for Organizational Resilience, BCM and Crisis Management have been reviewed and were ready for final approval and release by the Executive Directors at the

time of the publication of this report, pending any additional insights that could be gained through this audit assignment.

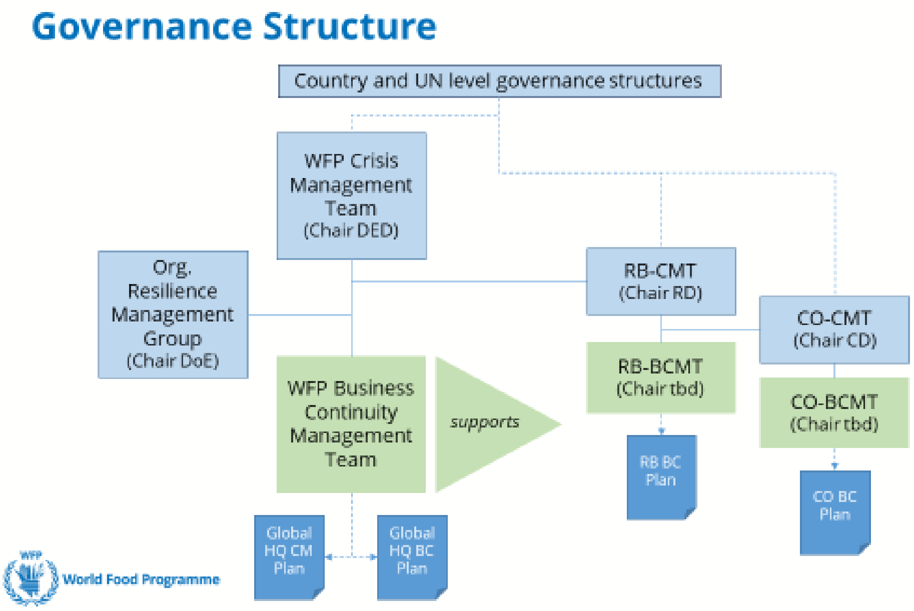
Governance

22. Effective and efficient BCM requires sponsorship by executive management; adequate human and financial resources; and effective governance mechanisms for its direction, evaluation and monitoring.

23. BCM encompasses several divisions, related functional areas and geographical dimensions (headquarters, RBs and COs). The 2016 BCM policy defines roles and responsibilities for the governance of BCM (see Figure 1). Policy amendments are needed to reflect differences between the BCM policy design and actual practices.

24. The BCM Team's role is to act as the secretariat for the CMT and ORMG; maintain the BCP; promote good practices in BC across the organization; and facilitate the integration of BCM with other WFP processes, such as Enterprise Risk Management (ERM) and EPRP. The ERM policy foresees the identification of risks, evaluating their impact in terms of "organizational resilience and continuity". The EPRP process, through the implementation of the Minimal Preparedness Actions (MPAs), aims to prepare COs to face emergencies better.

Figure 1: Governance structure



COVID-19 crisis management

25. On 24 February 2020, a corporate CMT was activated by the DED, to oversee WFP's response to the COVID-19 pandemic. At that time, supported by the BCM Team (as its secretariat) and the Operations Centre unit, the CMT was tasked with coordinating headquarters' response; analysing the pandemic's impact on WFP operations and the well-being of staff; and reviewing the solutions and contingency plans offered by WFP's BCP. As the pandemic evolved in Italy, on 17 March 2020, WFP headquarters decided to implement remote working for all its employees, with only essential location-dependent employees allowed on the premises.

26. On 30 March 2020, the Executive Director declared a Level 3 COVID-19 Response Corporate Surge Emergency directing WFP's global emergency response, supported by the Strategic and Operational Task Forces.

27. On 3 April 2020, the CMT's responsibilities for the COVID-19 response were redirected to WFP's headquarters, with the DED appointing the Director, Integrated Road Map as coordinator. The coordinator's specific focus was health, safety, security, travel, and BC solutions for headquarters and WFP's Office in Brindisi. The RBs were encouraged to form region-specific CMTs to enable prompt and contextual responses to the pandemic.

28. At the time of issuance of this report, the headquarters CMT and BCM Team continued to provide on-demand support and coordination to RBs and COs on implementation of BC activities, as required.

Objective and scope of the audit

29. The audit's objective was to provide assurance on the effectiveness of internal controls, governance and risk management processes related to BCM in WFP, and remote working arrangements in response to the COVID-19 pandemic (including connectivity, access to systems and data, and user support).[4] Such audits contribute to an annual and overall assurance statement provided to the Executive Director on governance, risk management and internal control processes.

30. The audit was carried out in conformance with the *Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing*. It was completed according to an approved engagement plan and considered the risk assessment exercise carried out before the audit.

31. The scope of the audit covered the period from 1 January to 31 August 2020. Where necessary, transactions and events pertaining to other periods were reviewed. The audit fieldwork took place from 12 October to 13 November 2020 at WFP headquarters in Rome.

32. A sample of six headquarters units and divisions, six RBs and eight COs were selected for a limited review.

33. International standards provide a framework for BCM, the most widely accepted being ISO 22301:2019,[5] which the audit used as a reference and a widely recognized benchmark of best practices. The scope of the audit encompassed the ISO 22301:2019 framework and included a COVID-19 specific procedure (Area 6):

- Area 1: Governance, Leadership oversight and Policies;
- Area 2: Risk Assessment and Business Impact Analysis;
- Area 3: Business Continuity and Disaster Recovery Strategies;
- Area 4: Operative Structures, Resources, Training and Awareness;
- Area 5: Planning, Testing, Monitoring, Evaluation and Improvement; and
- Area 6: COVID-19 Management and Remote Working Arrangements.

III. Results of the Audit

Audit work and conclusions

34. The audit reviewed the following to assess WFP's organizational resiliency, efficiency and effectiveness in BCM: organizational context; leadership; planning; support; operation; performance and evaluation; and improvement.

35. Based on the results of the audit, the Office of Internal Audit (OIGA) has come to an overall conclusion of **partially satisfactory / some improvement needed**[6]. The assessed governance arrangements, risk management and controls were generally established and functioning well but needed improvement to provide reasonable assurance that the objective of the audited entity/area should be achieved. Issue(s) identified by the audit were unlikely to significantly affect the achievement of the objectives of the audited entity/area. Management action is recommended to ensure that identified risks are adequately mitigated.

[4] A corporate Evaluation of WFP's Response to COVID-19 will cover workforce management, in complementarity to Internal Audit's coverage of the COVID-19 response in WFP.

[5] ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements

[6] See Annex B for definitions of audit terms.

Observations and actions agreed

36. Table 1 outlines the extent to which audit work resulted in observations and agreed actions. These are classified according to the areas in scope established for the audit and are rated as medium or high priority. Observations that resulted in low priority actions are not included in this report.

Table 1: Overview of areas in scope, observations and priority of agreed actions

	Priority of issues/agreed actions
A: Governance, leadership oversight and policies	
1 Governance structure and scope of WFP's Business Continuity Plans	*High*
B: Risk assessment and Business Impact Analysis	
2 Risk assessment supporting business continuity	*Medium*
3 Business Impact Analysis methodology and performance	*Medium*
C: Business Continuity and Disaster Recovery Strategies	
4 Business Continuity Plans	*Medium*
5 Disaster Recovery Plans	*Medium*
D: Operative structures, resources, training and awareness	
6 Business Continuity Management resources	*High*
7 Critical roles, training and awareness programmes	*Medium*
E: Planning, testing, monitoring, evaluation and improvement	
8 Planning, testing, monitoring and performance improvement	*High*
F: COVID-19 Management and remote working arrangements	
No observations raised	*N/A*

37. The observations of this audit are presented in detail below.

38. Management has agreed to take measures to address the reported observations.[7] An overview of the actions to be tracked by internal audit for implementation, their due dates and their categorization by WFP's risk and control frameworks can be found in Annex A.

[7] Implementation will be verified through the Office of Internal Audit's standard system for monitoring agreed actions.

A: Governance, leadership oversight and policies

39. The audit performed tests and reviews of existing policies for BCM and disaster recovery; supporting governance structure functions; allocation of resources; defined roles and responsibility; and monitoring and oversight mechanisms for BC activities.

40. According to the minimum requirements of ISO 22301:2019, *Management shall demonstrate leadership and commitment to the BCM systems in the organization*. The headquarters BCP specifies that crises and critical incidents will be headed by the CMT, chaired by the DED; the ORMG, chaired by the Director of Emergencies, leads the oversight and direction activities to ensure organizational resilience. The ORMG is expected to meet at least six times a year. The CMT chair has ultimate responsibility for approving the Crisis Management Plan, BCM Plans, and their updates. During activation of the BCP, the CMT can delegate responsibility to the ORMG as required. These governance structures are not mandatory at the RB and CO level. The BCM Team coordinates and supports best practice BC activities throughout the organization and supports the CMT and ORMG in discharging their duties.

Observation 1: Governance structure and scope of WFP's Business Continuity Plans

41. **Governance of BCM**: The ORMG last met in December 2017, leading to the CMT assuming responsibilities for crisis management when required. However, governance and leadership of BCM from Management should be a continuous process to evaluate, direct and monitor the efficiency, effectiveness and performance of BCM before crisis scenarios. Management and the CMT's limited involvement in BCM monitoring and oversight resulted in shortfalls of resources for BCM, and insufficient delegated authorities to the BCM Team going undetected.

42. **Scope of BCM**: Although there is no mandatory requirement for RBs and COs to have BCPs, they are encouraged to follow the corporate BCP template. Field offices were only required to prepare a BCPs for the COVID-19 response. All offices reviewed by OIGA had prepared BCPs in response to the COVID-19 pandemic; however, the BCPs were inconsistent in their content and level of completion, and the majority were still in draft form. The BCPs had not been approved by Management or supported by a formalized BIA and lacked critical sections including: description of impact scenarios; list of critical processes; lists of IT systems and staff; and communication protocols. Ten of the sampled BCPs were not structured around the three critical scenarios provided by the headquarters BCP: (i) no access to premises; (ii) devolution of critical business processes; and (iii) no access to systems. The RBs and COs reviewed acknowledged that, based on the lessons learned from the COVID-19 pandemic response, all WFP offices required comprehensive BCPs. The absence of a mandatory BCP requirement in field offices has led to gaps in WFP's preparedness level and its ability to respond and continue to deliver assistance to beneficiaries.

43. **Role of the BCM Team**: The BCM Team's role is not comprehensively defined in the BCP. Responsibilities for key BC activities such as planning, testing, implementation, monitoring and reporting are delegated to headquarters units, RBs or COs. The BCM Team provides coordination and support only when called upon, resulting in inconsistent tracking and oversight of BCM activities, especially in field offices. As a result, the BCM Team has a limited view of BCP implementation at the global level.

44. **Benchmarking WFP's BCM capacity**: A survey conducted in November 2020 by the Representatives of Internal Audit Services of the United Nations (UN RIAS), on the BCM practices of 27 United Nations and other international organizations, indicated that 67 percent of the organizations surveyed had staff managing BCM alongside other responsibilities, and only 19 percent had functions and teams dedicated to BCM. As a large organization, it is reasonable to expect that WFP would have a dedicated function/person managing BCM (as do 19 percent of survey respondents).

45. **Coordination and integration of BCM:** The organization has not reviewed the level of overlap and linkages in the BCM-related activities of the ERM division, the Emergency division and the BCM Team to identify opportunities for their integration. This review should improve the governance of BCM, and help support policy updates geared towards enhancing organizational resilience and preparedness.

46. Underlying cause(s): Relocation of BCM Team from the emergency unit that is designated to head the ORMG to the DED's office, diminishing the direct participation of the Emergencies division in BCM activities; BCP policy focused on headquarters; limited definition of the role of the BCM Team in the headquarters BCP; limited authority and resources for the BCM Team to establish centralized quality control, monitoring and oversight mechanism; and absence of formalized collaboration/coordination on BCM between the ERM division, the Emergency division and the BCM Team.

Proposed Agreed Action [High priority]

The Office of the DED, in consultation with the Directors of the Emergencies and the Enterprise Risk Management divisions and the BCM Team, will review and update WFP's BCM policies including consideration of: the scope of BCM policies to include RBs and COs; BCM objectives, to ensure objectives and requirements are coherent and mandatory at all levels of the organization; the role and continued relevance of the ORMG as a governance body, and the role of the ERM division in the governance and oversight of BCM; and the role and responsibilities of governance bodies, either directly or delegated, for directing, monitoring and evaluating BCM in WFP.

Timeline for implementation

30 September 2021

B: Risk assessment and Business Impact Analysis

47. The audit performed tests and reviews of the current risk assessment and BIA processes that support the BCPs. The review included the information in risk registers, BIAs and EPRPs prepared at headquarters, RBs and the sampled COs and a review of the linkages between the ERM policy, the EPRP guidelines and BCM systems. A periodic, at least yearly, update of the BIA is a minimum requirement under ISO 22301:2019 best practices and is mandated for WFP's headquarters by the BCP.

48. The headquarters BCP requires that the BIA basis be a risk assessment performed as directed by the ERM policy, which states that the impact of risks on WFP processes and objectives must consider the effect on *organizational continuity and resilience*, including safety and security for operational risks.

49. COs maintain a state of readiness and preparedness by implementing the MPAs as defined in the EPRP. The EPRP process focuses on mitigating the effects of contextual risks that can impact the continuity of operations. These include natural hazards, armed conflict, civil unrest, restrictive government legislation, socioeconomic environment changes, and terrorism. The EPRP risk assessment should not be independent of, nor parallel to, a CO's risk management process; instead, it is a tool to examine contextual risks and their impacts on WFP's internal and external environments and operations.

50. There is a growing awareness of cyber security risk in WFP, with 23 COs including cyber security in their 2020 risk registers. Cyber security campaigns, including mock phishing campaigns, advertising on the internal communication channel, and mandatory e-learning, were launched to raise users' awareness of cyber security risks from remote working. WFP staff members must complete mandatory cyber security training within two weeks of their appointment, with two advanced training modules released in November 2020.

Observation 2: Risk assessment supporting Business Continuity

51. The audit noted that the specific risks to WFP's BC were not consistently identified, analysed and formally assessed to support BIA and BCPs at various organization levels.

52. Processes linking the risks impacting operational continuity and resilience defined in the ERM policy to BIA and consequently BCPs were absent. The risk registers and BIAs reviewed by OIGA had not been consistently assessed using an identifiable and repeatable process. In seven of the eight sampled COs, there were significant differences between the risks identified in the risk registers and the EPRP tracking tool. Through the implementation of the MPAs, COs identify critical systems, business processes and staff. However, COs did not consistently use information from the MPA to perform and formalize BIA and BCPs.

53. Feedback received from sampled COs on the EPRPs indicated that:

- With the EPRP, COs did not see the need for a second process such as a BCP.
- In the absence of clear articulation between risk management processes, risk registers, the EPRP process and MPAs, there was a perception of duplication of content and effort.
- The COs perceived the EPRP process as onerous, and the BCP to be a less burdensome, more effective process to guarantee business resilience.

54. Procedures stipulated in the BCP may not be effective because the impact scenarios identified may not reflect specific BC threats already identified by the COs' risk assessment(s), and inconsistent evaluation of their severity.

Underlying cause(s): Limited coordination between the ERM division, BCM Team and EME division and absence of a clear process to assess and formalize the list of BC threats relevant for all WFP offices; and EPRP, BCP and ERM processes evolved separately, resulting in different stages of process maturity and lack of integration leading to duplication and misalignment of objectives and tools.

Proposed Agreed Action [Medium priority]

The Office of the DED and BCM Team, in reference to the agreed action in Observation 1, and in consultation with the Directors of Emergencies and Enterprise Risk Management divisions, will review and re-evaluate the objectives, risk management processes and tools used in the BCP, EPRP and risk register processes with the aim of developing a practical and synergistic approach to BCM.

Timeline for implementation

30 September 2021

Observation 3: Business Impact Analysis methodology and performance

55. A formalized, approved, and shared methodology for completing the BIA and identifying critical business processes and supporting IT systems is not defined in the current BCP. The current BIA has no specified criteria to evaluate business processes' criticality, existing IT systems and those undergoing development. For a sample of BIAs, including the "BCP toolkit" provided to COs, the minimum standard of information and criteria were missing to:

- Identify the relevant risk threatening BC to be considered in the BIA;
- Assess and rate the criticality of business processes;
- Identify the critical input, output and dependencies of business processes;
- Assess and evaluate IT systems' criticality supporting critical business processes (both existing and those undergoing development) and define Recovery Point Objective (RPO) requirements of critical IT systems;
- Identify the critical third parties involved in business processes and assess their BC preparedness; and
- After identifying and assessing the information above, define specific BC requirements of critical business processes and the critical IT systems.

56. The factors listed above make it difficult to consolidate the processes and IT requirements across WFP offices and departments in the BCP and Disaster Recovery Plan (DRP).

57. The headquarters BIA was last updated in 2016; it includes decommissioned IT systems and does not reflect new organizational entities such as the Staff Wellness division. Only two of eight headquarters divisions reviewed had updated their BIAs during the audit period, as a prerequisite to the devolution testing. The headquarters BCP requires the BIA to be updated annually; however, RBs and COs' BCPs did not indicate how often BIAs should be updated.

58. It is unclear what are the critical corporate processes to be included in the BCPs of all COs and RBs. The audit noted only one CO and three RBs with documented BIAs. The absence of a BIA results in an incomplete BCP in critical internal, external IT processes and resources.

Underlying cause(s): Unclear ownership and responsibilities for updating BIA activities; absence of a standardized approved methodology and guidelines, including a comprehensive reporting template for the performance and formalization of the BIA; lack of an effective monitoring and oversight mechanism for BC activities.

Proposed Agreed Action [Medium priority]

The BCM Team will develop and formalize guidelines that define the methodology, frequency, roles and responsibilities and reporting that COs should consider when performing, updating and formalizing their BIAs and BCPs.

Timeline for implementation

31 December 2021

C: Business Continuity and Disaster Recovery Strategies

59. The audit performed tests and reviews of the strategies defined in the BCP and DRP and supporting operational procedures. The review examined whether the strategies: (i) encompassed and integrated both organizational aspects and the IT systems and resources to support them; and (ii) were defined according to scenarios and relevant risks threatening BC as identified by the risk assessment and BIA processes.

60. Minimum requirements for an effective BCM system as per ISO 22301:2019 are adequate formalization of BC strategies and that supporting operational procedures are aligned to the risk assessment and BIA. The headquarters BCP strategy addresses how WFP manages the consequences of likely events threatening BC under three scenarios: no access to premises, devolution of critical business processes, and no IT systems access.

61. WFP established a BCM portal as a secondary repository in a separate facility and network domain to ensure the availability and access to critical procedures and information in case of an emergency. Access to the repository folders is roles-based and only provided to business-critical staff.

Observation 4: Business Continuity Plans

62. WFP offices (RBs and COs) were required to prepare or adjust existing BCPs in response to the COVID-19 pandemic, to facilitate a relevant response. Before the pandemic, BCPs were optional and were not in place in half of the RBs and two of seven COs sampled.

- The template provided in the "BCP toolkit" was not consistently utilized, leading to inconsistent or incomplete content.
- As indicated in Observation 2, impact scenarios may be incomplete and lack references or linkages to the scenarios identified in risk assessments (e.g. natural disasters, cyber-attacks, terrorism, etc.).
- Gaps in identifying relevant external interested third parties and formal communication protocols highly recommended by both ISO 22301 and best practices, can result in delays during a crisis.

63. The updates to critical processes and related BC procedures included in the eGuide and BC portal have not been consistent. The BCP did not include divisions created after its approval, nor were existing procedures regularly updated, leading to a risk that WFP does not have updated information on critical processes in the event of an emergency.

64. The India CO hosts three critical global services, including the IT Service Desk, Entitlement Travel unit, and Vendor Creation and Management unit. The formalization and approval of BC procedures for these services were paused due to the pandemic. The lack of BCP processes for these services may impact WFP's global BC response in the event of a disruptive incident in India.

Underlying cause(s): Absence of mandatory requirements for RBs and COs to have BCPs; absence of supporting guidelines for the "BCP toolkit" on required information to be included in the BCP, including guidelines on external communication; lack of a clear methodology to define impact scenarios using the information gathered during risk assessments; and limited authority and resources for the BCM Team to perform monitoring, oversight and quality control.

Proposed Agreed Actions [Medium priority]

The BCM Team will:

(a) In reference to the agreed action in Observation 1 and future scope of the BCPs, improve consistency and completeness of BCPs by RBs and COs, through guidance, support or other tools to support the "BCP toolkit" , including guidelines explaining the linkages between the BCP, relevant risk assessments and BIA.

(b) In collaboration with the relevant functional headquarters units and India CO, facilitate the formalization of BCPs for the global services encompassing WFP's IT Service Desk, Entitlement Travel unit, and Vendor Creation and Management.

Timeline for implementation

31 December 2021

Observation 5: Disaster Recovery Plans

65. During the review of the headquarters DRP, OIGA noted that:

- The DRP had not been updated since its approval in 2016, despite requirements for an annual update. The lack of periodic updates increases the risk that the DRP does not include all critical IT systems.
- The DRP lacks complete and consistent definitions of criticality, Recovery Time Objectives and RPOs due to incomplete BIAs (refer to Observation 2). The maximum tolerable duration of interruptions to corporate IT systems, and recovery prioritization, is not defined according to business requirements in the BIAs (at headquarters, RBs and COs levels). The absence of periodic reviews of DRPs and BIAs resulted in the misalignment of the critical systems identified in both headquarters documents.

66. Implementation of MPAs defined in the EPRP requires that COs have a DRP in place. While most of the sampled RBs and COs had DRPs, they were mainly focused on the provision of internet connectivity, given that most critical applications supporting their business processes are cloud-based and managed by headquarters. However, none of the sampled DRPs had defined procedures to support the resumption of operations at the primary facility, or to assess the recovered service after a failure.

Underlying cause(s): Lack of resources to monitor and support the relevance and update of DRPs; BIA process not periodically performed or updated, leading to issues in the design of the DRPs; and limited collaboration and coordination between the Technology division (TEC) and business units in the definition of BIA.

Proposed Agreed Actions [Medium priority]

The BCM Team will:

(a) In reference to the implementation of the agreed action for Observation 4, develop a monitoring and quality assurance mechanism for the performance and updating of BIAs and DRPs.

(b) Facilitate and coordinate TEC and business units' collaboration in the performance and updating of BIAs and DRPs.

Timeline for implementation

31 December 2021

D: Operative structures, resources, communication, training and awareness

67. The audit performed tests and reviews of: (i) resourcing and budgeting guidelines for BC activities; (ii) the current list of critical roles and attributed responsibilities attached to the BCP to verify that they are updated and coherent with the scope of critical processes identified; and (iii) training and awareness programmes to enhance BCM competencies and knowledge in the organization.

68. As a minimum requirement of ISO 22301:2019 and best practices, the definition of critical roles is fundamental for the continuity of critical activities in a disruptive incident. Therefore, clear criteria to identify and assess focal points' competencies and individuals in business-critical roles is imperative. A comprehensive and regular training programme should be provided and disseminated to all staff involved in critical roles. OIGA observed that the BCM Team had developed a training package supplied to BCM focal points, who are required to provide this training to critical staff in their respective business units.

69. As mentioned in Section B, COs are required to implement MPAs as defined in the EPRP. At the time of the audit, 70 percent of standard MPAs focused on operative structures such as providing emergency-related training to staff; gathering and documenting relevant contacts; and defining communication and emergency protocols.

Observation 6: Business Continuity Management resourcing

70. The BCM Team receives ad hoc funding from different headquarters units, including the DED's office. It is currently staffed with two employees, one of which also has responsibilities outside the BCM process. Investment cases submitted by the BCM Team, as recently as 2020, have been unsuccessful. The limited authority and resources given to the BCM Team constrain BCM coordination and monitoring activities.

71. Headquarters departments individually fund BCM operative activities without specific budget lines. Budgeting guidelines are not in place for RBs and COs on how to fund BC activities. As a result, RBs and COs were obliged to apply for emergency funding from various sources to pay for critical BC activities related to the COVID-19 pandemic. The current decentralized funding of BCM expenses does not enable the correct assessment, or a consolidated view, of funding needs and appropriation of funds for BCM, affecting the cost efficiency and effectiveness of BCM activities.

72. Based on the survey conducted by UN RIAS[8], the audit noted that 33 percent of United Nations system organizations had a dedicated BCM budget, compared to 37 percent that relied on ad hoc funding and 22 percent that had no budget allocation.

Underlying causes: Misalignment between expected activities and funding needs of the BCM Team and funding levels and resources allocated for BCM activities; and lack of funding guidelines or dedicated funding mechanisms to support BCM activities and related expenses.

[8] Survey of Business Continuity Management practices of 27 United Nations and other international organizations, conducted in November 2020 by UN RIAS.

Proposed Agreed Actions [High priority]

1. The DED's office will assess, define and facilitate the approval of:

   a. Regular funding to support ongoing BCM activities including coordination, support, monitoring, oversight and reporting.

   b. A centralized funding facility to fund organization-wide (headquarters, RBs and COs) BCM-related expenses in the event of an emergency or disruptive incident.

2. The BCM Team, in consultation with the Budget and Programming division, will define a list of criteria or key BCM-related activities that each level of the organization (headquarters, RBs and COs) should consider in budgeting for these expenses; and issue supporting guidelines.

Timeline for implementation

30 June 2021

Observation 7: Critical roles, training and awareness programmes

73. Senior staff directly responsible for executing critical processes are selected as BCM focal points to ensure the highest technical knowledge level for BCM purposes. Guidance from the BCM Team also indicates it is preferable to appoint non-rotational staff as BCM focal points to ensure continuity. However, a formal process for assessing the business-critical appointed staff and map their competency and training needs was not in place to close BCP-related gaps. Best practices under ISO 22301 call for organizations to "retain appropriate documented information as evidence of competence", including "actions to acquire the necessary competence" and "to evaluate the effectiveness of the actions taken".

74. Training for BCM-related activities, such as devolution of BCP processes and focal points, were not consistently performed. The COs sampled by the audit had not planned regular BCM training activities. Some exercises were carried out in 2020 without supporting learning and training sessions and were further interrupted by the COVID-19 pandemic.

75. The BCM Team provides a brief presentation that introduces BCM focal points to WFP's BCM systems; however, additional tailored training material related to BCM processes was not provided, nor were awareness campaigns developed to reinforce BCM. The training required by the EPRP MPAs is limited to emergency procedures and does not include BCPs. As noted by the audit's COs, WFP offices do not have specific funds and resources dedicated to BCM activities.

76. Inadequate training impacts the effectiveness of BCM activities, including devolution of responsibilities. Lack of training for focal points and critical staff has resulted in limitations in discharging their roles and responsibilities, especially in COs.

Underlying cause(s): Absence of periodic processes to assess BCM focal point and critical staff's competency and training needs; limited involvement by business units; and lack of resources available to the BCM Team and business units to develop, define and implement comprehensive training packages.

Proposed Agreed Action [Medium priority]

The BCM Team will formalize criteria for selecting critical staff and BCM focal points, including the skill set and competencies to be assessed; and, pending the allocation of funds based on agreed actions for observation 6, will develop and coordinate the delivery BCM training and awareness programmes.

Timeline for implementation

31 December 2021

E: Planning, testing, monitoring, evaluation and improvement

77. The audit performed tests and reviews of plans for implementing BCP activities; tests by WFP of BCP and DRP procedures; monitoring and results from evaluating these activities; and any remedial actions approved by Management.

78. Periodic, consistent and complete testing of BCP and DRP procedures are essential to:

- Assure BC strategies and operative arrangements' adequacy and effectiveness to mitigate risks threatening BC, with the business's requirements;
- Monitor the performance of the BC strategies over time as defined by the BCP and DRP; and
- Detect existing gaps and misalignments between BC strategies and the requirements identified by the business.

79. WFP is implementing cloud computing. As noted by OIGA in its Internal Audit of Cloud Computing in WFP[9], contracts with cloud service providers include high availability clauses. These clauses allow WFP to request that a predefined number of data recovery tests are performed annually, or verify that the provider performs these autonomously.

Observation 8: Planning, testing, monitoring and performance improvement

80. **Test plan:** A formalized plan for coordinating the testing, monitoring and performance of both BCP and DRP activities is not in place. Testing activities are decentralized and delegated to individual business units, which are not obliged to involve the BCM Team and TEC. While the BCM Team plays an oversight role in the testing BCPs, the lack of direct involvement of TEC and the BCM Team increases the risk that testing is insufficient and inconsistent.

81. **Testing, results and formalization:** The testing of critical processes in the devolution model defined in the headquarters BCP is not complete. During the audit period, testing for certain business processes was performed but not completed. Only two critical IT systems have been tested since the inception of the BCP and DRP, and only once, while WFP never tested two critical BCP backup systems. The global services based in India, including Entitlement Travel, IT Helpdesk, and Vendor Creation and Management, have informal BC and devolution plans which had never been tested for BC before the COVID-19 pandemic. Structured testing of the BCP and DRP was completed for headquarters. RBs and COs lacked testing plans or reports to review results. Current BCM documentation does not define (i) a testing template for both BC procedures and Disaster Recovery (DR) testing; (ii) the minimum set of information to be reported; and (iii) the person responsible in the functional unit to collate this information.

82. **Review and evaluation of testing results:** Management did not periodically review the BC and DR exercises results or establish a process to review lessons learned and approve remedial actions for implementation. The follow-up of actions was independently tracked by each responsible functional unit or office, diminishing the process's visibility and accountability. Evaluation criteria for DR testing were not entirely based on the recovery parameters of IT systems resulting from the BIA. Moreover, there was a misalignment between the incomplete BIA's recovery parameters and the actual parameters used in WINGS DR testing and evaluation.

83. **Monitoring and performance improvement:** BCM Key Performance Indicators (KPIs) have not been formally defined and monitored, including KPIs for BIA updates; the scope of test plans; scope and level of execution; and BC training and awareness campaigns. The current headquarters BCP does not assign responsibilities for monitoring the test's performance and gathering test results and analyses to produce comprehensive BCM KPIs.

[9] Internal Audit of Cloud Computing in WFP, Office of Internal Audit, AR/20/09 (March 2020).

Underlying cause(s): Limited authority and resources for the BCM Team to perform key BCM activities such as planning, monitoring and evaluation; absence of guidance to define the formalization of BC exercises; and limited involvement at an operative level of Management to set KPIs, and direct, monitor and evaluate BCM activities.

Proposed Agreed Actions [High priority]

The BCM Team will:

(a) With reference to agreed actions in observations 1 and 6 respectively, align the Team's roles and responsibilities for coordination, consolidation and facilitation of the planning, testing, monitoring and oversight of the BCP to the updated BCM policies and guidelines; provide monitoring and oversight of the DRP.

(b) Develop KPIs for BCM to be approved by relevant governance bodies as per observation 1, and processes for the periodic measurement and reporting of BCM.

Timeline for implementation

31 December 2021

F: COVID-19 Management and remote working arrangements

84. The audit performed tests and reviews of WFP's management response to the COVID-19 pandemic, focusing on remote working arrangements at headquarters, RBs and the sampled COs (including connectivity, access to systems and data, and user support). The audit reviewed: (i) the processes for mapping critical and non-critical personnel and processes and the implications for working arrangements; (ii) processes that facilitate remote working (both from a procedural and IT equipment perspective); (iii) access to office facilities; and (iv) safety and security measures for staff and beneficiaries.

85. The audit noted the following positive aspects:

- All the sampled offices had appointed a CMT (or equivalent crisis-response body) that effectively directed and oversaw the response to the COVID-19 pandemic.
- Remote working arrangements brought about by the COVID-19 pandemic were successfully supported by WFP's investment in digitization and adoption of cloud-based computing of critical IT systems, enhancing overall organizational resilience.
- The increased requests for IT support (+60) resulting from the surge in remote working were adequately and promptly managed, with minimal adjustments to existing IT Service Helpdesk resources.
- Most COs had completed remote working simulations before the COVID-19 surge, learning from the experience of the pandemic's evolution in Europe and addressing emerging issues to ensure that employees could work remotely without interruption.
- Headquarters provided prompt guidelines for the COVID-19 response, which were adapted to the context of RBs and COs, allowing them to manage the continuity of their operations during the pandemic.

86. The audit review did not find any significant observations in this area.

Annex A – Summary of observations

The following tables show the categorization, ownership and due date agreed with the auditee for all the audit observations raised during the audit. This data is used for the macro analysis of audit findings and monitoring the implementation of agreed actions.

High priority observations		**Categories for aggregation and analysis:**			**Implementation lead**	**Due date(s)**
		WFP's Internal Audit Universe	**WFP's Governance, Risk & Control logic:**			
			Risks (ERM)	**Processes (GRC)**		
1	Governance structure and scope of WFP's Business Continuity Plans	Business Continuity Management	Governance & oversight risks	Preparedness	DED	30 September 2021
6	Business Continuity Management resourcing	Business Continuity Management	Governance & oversight risks	Preparedness	DED BCM	30 June 2021
8	Planning, testing, monitoring and performance improvement	Business Continuity Management	Business process risks	Risk management	BCM	31 December 2021

Medium priority observations		**Categories for aggregation and analysis:**			**Implementation lead**	**Due date(s)**
		WFP's Internal Audit Universe	**WFP's Governance, Risk & Control logic:**			
			Risks (ERM)	**Processes (GRC)**		
2	Risk assessment supporting business continuity	Business Continuity Management	Business process risks	Risk management	DED	30 September 2021
3	Business Impact Analysis methodology and performance	Business Continuity Management	Business process risks	Risk management	BCM	31 December 2021
4	Business Continuity Plans	Business Continuity Management	Business process risks	Risk management	BCM	31 December 2021
5	Disaster recovery plans	Business Continuity Management	Business process risks	Risk management	BCM	31 December 2021
7	Critical roles, training and awareness programmes	Business Continuity Management	Business process risks	Risk management	BCM	31 December 2021

Annex B – Definitions of audit terms: ratings & priority

1 Rating system

The internal audit services of UNDP, UNFPA, UNICEF, UNOPS and WFP adopted harmonized audit rating definitions, as described below:

Table B.1: Rating system

Rating	Definition
Effective / satisfactory	The assessed governance arrangements, risk management and controls were adequately established and functioning well, to provide reasonable assurance that issues identified by the audit were unlikely to affect the achievement of the objectives of the audited entity/area.
Partially satisfactory / some improvement needed	The assessed governance arrangements, risk management and controls were generally established and functioning well but needed improvement to provide reasonable assurance that the objective of the audited entity/area should be achieved. Issue(s) identified by the audit were unlikely to significantly affect the achievement of the objectives of the audited entity/area. Management action is recommended to ensure that identified risks are adequately mitigated.
Partially satisfactory / major improvement needed	The assessed governance arrangements, risk management 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. Issues identified by the audit could negatively affect the achievement of the objectives of the audited entity/area. Prompt management action is required to ensure that identified risks are adequately mitigated.
Ineffective / unsatisfactory	The assessed governance arrangements, risk management and controls were not adequately established and not functioning well to provide reasonable assurance that the objectives of the audited entity/area should be achieved. Issues identified by the audit could seriously compromise the achievement of the objectives of the audited entity/area. Urgent management action is required to ensure that the identified risks are adequately mitigated.

2 Priority of agreed actions

Audit observations are categorized according to the priority of agreed actions, which serve as a guide to Management in addressing the issues in a timely manner. The following categories of priorities are used:

Table B.2: Priority of agreed actions

High	Prompt action is required to ensure that WFP is not exposed to high/pervasive risks; failure to take action could result in critical or major consequences for the organization or for the audited entity.
Medium	Action is required to ensure that WFP is not exposed to significant risks; failure to take action could result in adverse consequences for the audited entity.
Low	Action is recommended and should result in more effective governance arrangements, risk management or controls, including better value for money.

Low priority recommendations, if any, are dealt with by the audit team directly with Management. Therefore, low priority actions are not included in this report.

Typically audit observations can be viewed on two levels: (1) observations that are specific to an office, unit or division; and (2) observations that may relate to a broader policy, process or corporate decision and may have broad impact.

To facilitate analysis and aggregation, observations are mapped to different categories.

3 Categorization by WFP’s audit universe

WFP’s audit universe[10] covers organizational entities and processes. Mapping audit observations to themes and process areas of WFP’s audit universe helps prioritize thematic audits.

Table B.3: WFP’s 2019 audit universe (themes and process areas)

A	Governance	Change, reform and innovation; Governance; Integrity and ethics; Legal support and advice; Management oversight; Performance management; Risk management; Strategic management and objective setting.
B	Delivery	(Agricultural) Market support; Analysis, assessment and monitoring activities; Asset creation and livelihood support; Climate and disaster risk reduction; Emergencies and transitions; Emergency preparedness and support response; Malnutrition prevention; Nutrition treatment; School meals; Service provision and platform activities; Social protection and safety nets; South-south and triangular cooperation; Technical assistance and country capacity strengthening services.
C	Resource Management	Asset management; Budget management; Contributions and donor funding management; Facilities management and services; Financial management; Fundraising strategy; Human resources management; Payroll management; Protocol management; Resources allocation and financing; Staff wellness; Travel management; Treasury management.
D	Support Functions	Beneficiary management; CBT; Commodity management; Common services; Constructions; Food quality and standards management; Insurance; Operational risk; Overseas and landside transport; Procurement – Food; Procurement - Goods and services; Security and continuation of operations; Shipping - sea transport; Warehouse management.
E	External Relations, Partnerships and Advocacy	Board and external relations management; Cluster management; Communications and advocacy; Host government relations; Inter-agency coordination; NGO partnerships; Private sector (donor) relations; Public sector (donor) relations.
F	ICT	Information technology governance and strategic planning; IT Enterprise Architecture; Selection/development and implementation of IT projects; Cybersecurity; Security administration/controls over core application systems; Network and communication infrastructures; Non-expendable ICT assets; IT support services; IT disaster recovery; Support for Business Continuity Management.
G	Cross-cutting	Activity/project management; Knowledge and information management; M&E framework; Gender, Protection, Environmental management.

4 Categorization by WFP’s governance, risk & compliance (GRC) logic

As part of WFP’s efforts to strengthen risk management and internal control, several corporate initiatives and investments are under way. In 2018, WFP updated its Enterprise Risk Management Policy[11], and began preparations for the launch of a risk management system (Governance, Risk & Compliance – GRC – system solution).

As a means to facilitate the testing and roll-out of the GRC system, audit observations are mapped to the new risk and process categorizations as introduced[12] by the Chief Risk Officer to define and launch risk matrices, identify thresholds and parameters, and establish escalation/de-escalation protocols across business processes.

[10] A separately existing universe for information technology with 60 entities, processes and applications is currently under review, its content is summarised for categorization purposes in section F of table B.3.

[11] WFP/EB.2/2018/5-C.

Table B.4: WFP's new ERM policy recognizes 4 risk categories and 15 risk types

1	Strategic	1.1 Programme risks, 1.2 External Relationship risks, 1.3 Contextual risks, 1.4 Business model risks
2	Operational	2.1 Beneficiary health, safety & security risks, 2.3 Partner & vendor risks, 2.3 Asset risks, 2.4 ICT failure/disruption/attack, 2.5 Business process risks, 2.6 Governance & oversight breakdown
3	Fiduciary	3.1 Employee health, safety & security risks, 3.2 Breach of obligations, 3.3 Fraud & corruption
4	Financial	4.1 Price volatility, 4.2 Adverse asset or investment outcomes

Table B.5: The GRC roll-out uses the following process categories to map risk and controls

1	Planning	Preparedness, Assessments, Interventions planning, Resource mobilization and partnerships
2	Sourcing	Food, Non-food, Services
3	Logistics	Transportation, Warehousing
4	Delivery	Beneficiaries management, Partner management, Service provider management, Capacity strengthening, Service delivery, Engineering
5	Support	Finance, Technology, Administration, Human resources
6	Oversight	Risk management, Performance management, Evaluation, Audit and investigations

5 Monitoring the implementation of agreed actions

The Office of Internal Audit tracks all medium and high-risk observations. Implementation of agreed actions is verified through the Office of Internal Audit's system for the monitoring of the implementation of agreed actions. The purpose of this monitoring system is to ensure management actions are effectively implemented within the agreed time frame to manage and mitigate the associated risks identified, thereby contributing to the improvement of WFP's operations.

OIGA monitors agreed actions from the date of the issuance of the report with regular reporting to senior management, the Audit Committee and the Executive Board. Should action not be initiated within a reasonable timeframe, and in line with the due date as indicated by Management, OIGA will issue a memorandum to Management informing them of the unmitigated risk due to the absence of management action after review. The overdue management action will then be closed in the audit database and such closure confirmed to the entity in charge of the oversight.

When using this option, OIGA continues to ensure that the office in charge of the supervision of the unit who owns the actions is informed. Transparency on accepting the risk is essential and the Risk Management division is copied on such communication, with the right to comment and escalate should they consider the risk accepted is outside acceptable corporate levels. OIGA informs senior management, the Audit Committee and the Executive Board of actions closed without mitigating the risk on a regular basis.

Annex C – Acronyms

BC	Business Continuity
BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CMT	Crisis Management Team
CO	Country Office
COVID-19	Coronavirus Disease
DED	Deputy Executive Director
DR	Disaster Recovery
DRP	Disaster Recovery Plan
EPRP	Emergency Preparedness Response Package
ERM	Enterprise Risk Management
GRC	Governance, Risk and Compliance
IT	Information Technology
JIU	Joint Inspection Unit
KPI	Key Performance Indicator
MPA	Minimum Preparedness Action
OIGA	Office of Inspector General Internal Audit
ORMG	Organizational Resilience Management Group
ORMS	Organizational Resilience Management Systems
RB	Regional Bureau
RBs	Regional Bureaus
RPO	Recovery Point Objective
TEC	Technology division in WFP
UN RIAS	United Nations Representatives of Internal Audit Services
WFP	World Food Programme