SAVING
LIVES
CHANGING
LIVES

Internal Audit of ICT Management in Country Offices

Office of the Inspector General
Internal Audit Report AR/19/10

WFP
World Food
Programme

May 2019

Contents

Internal Audit of ICT Management in Country Offices

I. Executive Summary

1. As part of its annual work plan, the Office of Internal Audit conducted an audit of information and telecommunications management in WFP country offices. The audit was performed using a structured questionnaire on a sample of 18 country offices, three from each region, to perform a desk review that focused on the period from 1 January 2016 to 31 March 2018. Where necessary, transactions and events pertaining to subsequent periods were reviewed. Fieldwork was performed at six country offices, one from each region, and took place during the period from 10 July to 31 October 2018. The audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing*.

2. The Technology Division, based in WFP headquarters, Rome, is responsible for the technology and communications infrastructure within WFP, providing services and support to some 14,700 WFP staff, of which 90 percent work outside Rome headquarters in 83 country offices and six regional bureaux. The Technology Division has oversight and enforcement responsibility for the application of relevant policies, standards and management practices in WFP headquarters in Rome, and in the field, supported by Regional Information Technology Officers.

3. Four main lines of enquiry were established for the audit:

(a) Governance and management oversight over the information and communications technology (ICT) function in field locations;

(b) Planning for ICT resources and their management;

(c) Logical and physical security mechanisms; and

(d) Continued information technology (IT) services, user support, documentation and training.

Audit conclusions and key results

4. 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, but needed 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. The audit report contains one high priority and five medium priority observations, all of which have agreed actions directed at the corporate level. The agreed actions identify the Technology Division as the primary lead for implementation; most actions require the cooperation and support of various other parties at the headquarters, regional and country office level, under the sponsorship of the Management Information Systems Steering Committee.

5. The audit noted that, while generally functioning, the ICT function presented inconsistent governance, structure and management in the country offices reviewed. While WFP's Human Resources and Technology Divisions are working on aligning resources to functional requirements, country offices did not identify the required IT support to the Country Strategic Plan objectives and address issues that required medium- to long-term planning to fully resolve; risks were not escalated; and there was no service-level agreement between the headquarters, regional and country level. The representation of the country offices needs and issues in the Management Information Systems Steering Committee and in the decision-making for ICT

solutions was insufficient. Lack of clear interlinkages between ICT and digital objectives in countries and at headquarters resulted in some disconnect between the objectives and capacity in the field and the support and implementation of corporate objectives, with a risk of inefficiencies, duplication and/or a risk to the continuity of the operations. Further integration would help ensure an effective implementation of WFP's digital strategy.

6. ICT resources in the field should be managed in a way that supports the operations of the respective office in a cost-effective way. There were no criteria at the corporate and regional level to help determine the number, skills and competencies of IT staff in country, leading to a wide disparity in the IT staff to user ratio between offices. Some of the smaller in-country IT units faced challenges in supporting corporate applications such as SCOPE, implementing IT projects initiated by various business units or managing a large inventory of ICT assets.

7. Wide disparities between the results of physical counts and records and the accumulation of old, obsolete and missing items that needed to be written off have built up over a number of years. The absence of up-to-date standard operating procedures covering the entire process of acquisition, transfer, monitoring and disposal of ICT assets was a major contributing factor. The administration of access, including for personal devices, and segregation of duties for WFP's enterprise resource planning system required further clarification and structure in its management.

8. The ICT function was responsible for maintaining plans for the recovery and restoration of the IT systems and to keep them effective through regular testing. IT disaster recovery plans had not been recently updated and tested. Under the revised corporate guidelines, it was no longer mandatory for country offices to have a business continuity plan distinct from the emergency preparedness response package, the focus of which is safeguarding people from harm. There was a need to revisit and review the process, starting with a business impact analysis and risk assessment.

Actions agreed

9. Management has agreed to address the reported observations and work to implement the agreed actions by their respective due dates. An overview of all observations and agreed actions is provided in Table 1.

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

Kiko Harvey

Inspector General

II. Context and Scope

Management of Information and Communications Technology in the Field

11. WFP has 83 country offices (CO), with six regional bureaux (RBs) providing oversight and support services. The Technology Division (TEC), based in WFP headquarters, Rome, is responsible for the information and communications technology (ICT) infrastructure within WFP, providing support to staff and operations through three main channels: user services, business solutions and IT partner services. TEC takes the lead in establishing the corporate policy for ICT and has oversight and enforcement responsibility for the application of relevant policies, standards and management practices in headquarters and in the field.

12. TEC employs 85 regular staff at headquarters. A further 800 staff are employed by COs worldwide to support the management of ICT in the field. TEC's day-to-day operations are managed by a Chief Information Officer (CIO), supported by a Deputy and Chiefs of Branches that cover the major components of the TEC domain. These include beneficiary services, service management, resource management, information security, and emergency preparedness and response. TEC also has an architecture, engagement and delivery group for ICT solutions that comprises business engagement, architecture and digital solution delivery.

13. Regional Information Technology Officers (RITOs) are located in the RBs and form part of the TEC management team, with a functional reporting line to the Deputy Chief Information Officer. RITOs report to RB senior management and provide a two-way communication with the IT units in the field. The office of the RITO has an oversight role to ensure COs comply with corporate IT policies and standards, and IT risks to CO operations are effectively mitigated.

14. ICT staff in COs, under the supervision of the country director, provide direct support to WFP operations in the field, enabling connectivity to WFP's corporate systems, managing communication with deep field offices and ICT equipment, and filing the gap for information system solutions not served by corporate systems.

15. TEC targets to align its people, processes and technology to the business capabilities identified by the business units and field offices and achieve WFP's digital transformation agenda depends in large part on a framework that enables countries to develop information systems to fill specific IT needs currently not served by corporate systems and connectivity to make effective the implementation of new technologies such as SCOPE.

Objective and scope of the audit

16. The objective of the audit was to evaluate and test the adequacy and effectiveness of the processes associated with the internal control components of ICT management in WFP country offices. Such audits are part of the process of providing an annual and overall assurance statement to the Executive Director on governance, risk-management and internal control processes.

17. 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 took into consideration the risk assessment exercise carried out prior to the audit.

18. The audit was conducted using a structured questionnaire on a sample of 18 COs, three from each region, to perform a desk review that focused on the period 1 January 2016 to 31 March 2018. Where necessary, transactions and events pertaining to other periods were reviewed. Fieldwork was performed in Chad, Ethiopia, Honduras, Malawi, Pakistan and Sudan and took place during the period 10 July to 31

October 2018 at WFP headquarters. In October, a questionnaire was used to obtain information and comments from the RITOs. Work at headquarters focused on connectivity and a review of relative corporate policies, standards and guidelines.

III. Results of the Audit

Audit work and conclusions

19. The audit was tailored to the context and to the objectives set by WFP for the management of ICT in COs, taking into consideration the corporate and selected CO and RB risk registers, findings of WFP's second line of defence functions, as well as an independent audit risk assessment.

20. Based on the results of the audit, the Office of Internal Audit has come to an overall conclusion of **Partially satisfactory / Some improvement needed**[1]. The assessed governance arrangements, risk management and controls were generally established and functioning, but needed 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. The Office of Internal Audit, in supporting WFP's management's ongoing efforts in the areas of risk management and data quality, separately reports its assessments or gaps identified in both areas.

Risk management maturity

21. High risks tended to be common across the regions, the topmost being cybersecurity, outdated and unstable IT infrastructure, staffing, numbers and skills, and change management. An accurate risk landscape at the CO level is an important contributor to the landscape at the regional and global levels, with adequate escalation and consolidation at the regional and corporate level, also informing the directions of TEC and support to be provided by RITOs or headquarters.

Data quality

22. Automation was needed to improve ICT asset data in WFP's Global Equipment Management System (GEMS) to ensure asset movements, and end-of-life cycle data fields did not remain dependent on the results of asset physical counts.

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

Observations and actions agreed

Table 1 outlines the extent to which audit work resulted in observations and agreed actions. These are rated as low, 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
Line of enquiry 1: Is there a well-defined mechanism for governance and management oversight over the ICT function in field locations that clearly identifies the business process owners' responsibilities and minimizes WFP's IT risk exposure?	
1. Governance and strategic planning	Medium
2. Structure, positioning and responsibilities of the ICT function	Medium
Line of enquiry 2: Is planning for ICT resources and their management adequate to ensure users are provided with the ICT systems and resources to perform their duties in the most efficient way?	
3. Planning and managing the delivery and maintenance of local IT solutions	Medium
4. Management of ICT assets	Medium
Line of enquiry 3: Are effective logical and physical security mechanisms in place to prevent unauthorized access to programs, data and computer installations, and detect any violation of security?	
5. Administration of security access, use of personal devices and segregation of duties in WINGS	Medium
Line of enquiry 4: Are users provided with continued IT services, support, documentation and training to enable them to use the systems correctly and effectively?	
6. Manage continuity	High

23. The six observations of this audit are presented in detail below.

24. Management has agreed to take measures to address the reported observations.[2] 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.

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

Line of enquiry 1: Is there a well-defined mechanism for governance and management oversight over the ICT function in field locations that clearly identifies the business process owners' responsibilities and minimizes WFP's IT risk exposure?

The audit reviewed the governance and oversight framework for ICT management in COs, including mechanisms and authorities to enable the governance requirements to be met, the establishment and communication to COs of corporate ICT policies, the establishment of local policies or standard operating procedures (SOPs) where required, and the monitoring of compliance with such policies and SOPs. It assessed whether the roles and responsibilities of ICT personnel and other stakeholders with responsibilities for ICT were clearly established and properly exercised, and whether significant ICT responsibilities, including application development, were being exercised by units within the CO, independent of the ICT unit. The audit reviewed the mechanism employed by COs for prioritizing the allocation of ICT resources and managing an ICT budget. It looked at the criteria being used to determine the number, skills and competencies of ICT staff and the tools employed for staff learning and development. The audit looked at the ICT-related performance measures in place and the role of the RITO, the criteria for missions for oversight purposes and the reports from missions performed since 1 January 2016.

In most of the COs, the ICT function was well-represented in the CO governance and management structure, with the head of the ICT unit reporting to the country director or deputy country director and participating in meetings of the senior management team. IT units demonstrated an awareness of the relevant corporate ICT policies. The relationship between the IT units with the respective RITO was positive with input to the CO ICT work plans and regular meetings for informative and consultative purposes. Through their reporting line and meetings with the TEC Director, RITOs provided timely advice and guidance on policy and procedural matters and updates on corporate ICT initiatives. Problems were escalated through the RITO and technical support for specialized areas provided on a request basis. During the review period, five out of the 18 sampled COs requested the RITO to perform an on-site review and assessment on subjects such as network performance, connectivity, local internet service providers and SCOPE. RITOs have been instrumental in setting up a number of active Emergency Telecommunication Clusters (ETC) and Emergency Telecommunication Sector initiatives with other United Nations agencies.

RITOs are part of the TEC management team, reporting to RB senior management with a functional reporting line to the deputy CIO. RITOs have an oversight role for compliance with corporate IT policies and standards and ensure IT risks are effectively mitigated. During the period 1 January 2016 to 31 October 2018, RITOs conducted 55 oversight missions. In 2018, these took place in nine of the 18 COs sampled by the audit. The Field IT Compliance and Risk Management System (FIT-CRM) provided a methodology to determine the frequency of oversight activities, although not consistently used across the regions. Findings and recommendations were linked to risks, but not to the relevant criteria from corporate policies, standards or guidelines.

Observation 1	**Agreed actions [**Medium priority**]**
Governance and strategic planning From a strategic perspective, there was no clear plan for ICT and how technology was to support the CO's short to medium term directions, in alignment with the corporate ICT strategy and digital transformation agenda. The audit noted that this affected the rightsizing of the ICT infrastructure and resourcing, including non-adherence to corporate policies, such as those for locally acquired IT solutions, continuity management, and the ability of WFP to evaluate cyber security risks when engaging service providers and cooperating partners for cash-based transfers or programme implementation. Service Level Agreements between regional or corporate levels with COs were not formalized to define the direction and expected level of support. IT units escalated critical issues to TEC via the RITO or, for specific projects such as network assessments, directly to the TEC focal point. Better articulation of the digital and technology priorities at HQ, regional and country level would ensure countries are equipped for digital transformation.COs invested time and resources in developing IT solutions. While such flexibility is a key feature of WFP's digital agility, the lack of visibility and quality control over locally	1. TEC will: (i) Clarify existing governance guidelines in the IT manual, identifying practical governance mechanisms at the CO-level to align business and IT interests; (ii) Update the 2015 Governance and Management Framework for Field IT, in line with changes to WFP's ICT environment; (iii) Analyse COs IT needs and directions at the regional and corporate levels to ensure alignment with the corporate IT strategy, and

Observation 1	**Agreed actions [**Medium priority**]**
developed IT solutions is a risk that OIGA already highlighted in prior reviews[3]. As these were not known let alone made available to other COs, there is duplication of efforts. For example, up to six IT service management solutions have been developed in 14 of the COs sampled by the audit. WFP's IT assets inventory system (GLASS) did not provide a complete picture of locally developed solutions. As controls over the development and maintenance of locally developed solution may not meet corporate requirements, the cybersecurity risk is increased for business continuity, data privacy and protection, etc. The RITOs oversight missions did not cover areas such as shadow IT and digital transformation. OIGA's audit of COMET[4] highlighted the need to better consider the needs of COs in terms of system solutions, integration and simplification. There is also no representation of COs in the Management Information Systems Steering Committee (MISSC). A regional director is appointed to represent field operations at MISSC; however, it is not clear how the information received by the RITOs is channeled and coordinated with this representation. Nine of the 18 COs surveyed used key performance indicators (KPIs) as identified in the 2015 Governance and Management Framework for Field IT. Five offices used indicators such as connectivity capacity and end-user devices. Four used satisfaction survey. Without common KPIs management in RBs and TEC may not be able to timely and effectively identify and address issues. While regional oversight missions from the RITOs took place in nine of the 18 sampled countries, COs were not mandated to track or implement oversight recommendations, and none of the reports provided an implementation timeline. The audit noted that a high rate of recommendations had not been implemented or were still in progress at the time of the audit. There is a risk that weaknesses identified are not addressed timely and that oversight missions are not seized as opportunities to mitigate IT risks. We noted that WFP's Enterprise Risk Management Division (RMR) is in the process of developing a corporate risk management and oversight recommendation tracking tool which will house oversight recommendations and management responses in a single platform, including second line recommendations, allowing for greater visibility and effective monitoring of these at the CO, regional and corporate levels. <u>Underlying causes:</u> Absence of corporate policies that defined the ICT governance structure with the field and provided guidance on strategic planning at the CO level. Reference guideline not updated in line with the corporate IT strategy and changes in WFP's ICT environment. Disconnect between corporate and CO-driven ICT initiatives, field priorities and needs and related business process transformation required for their implementation. Absence of escalation of critical IT risks at the CO level. Inconsistent use of KPIs. No centralized system for tracking implementation by COs of recommendation coming from second line of defence oversight. Corporate risk management and oversight tools are being implementation but have not yet been rolled out.	alignment between ICT corporate strategies and initiatives to the COs ICT organizational capacities; (iv) Identify gaps in guidelines for ICT management in CO, and survey and select common tools and SOPs from the ones already developed for adoption at a corporate level; and 2. The Chair of the MISSC will review the composition of the committee to ensure adequate representation of COs, considering different options to capture CO inputs into WFP's IT audit strategy. These mechanisms may include a sub-committee representing COs, and/or improved communications between the MISSC and field operations. 3. RMR will provide a technical solution for tracking recommendations in the Governance Risk and Control system that is flexible enough to accommodate recommendations from various sources, including the second line of defense. RMR will liaise with TEC as the functional owner of RITO recommendations about to encourage tracking these in the GRC system.

[3] Advisory on cybersecurity, audit of IT Governance and Monitoring.

[4] *Internal Audit of the Development and Delivery of COMET* (Country Office Tool for Managing - programme operations – Effectively), Internal Audit Report AR/19/02, WFP's Office of the Inspector General.

Observation 2	**Agreed actions [**Medium priority**]**
Structure, staffing and responsibilities of the ICT function ***Reporting lines*** – In 2015, TEC drafted the Governance and Management Framework for Field IT, recommending a structure where the head of IT reports to the country director or the deputy country director. Such structure was implemented in only two COs. Seven CO ICT functions reported to the Head of Finance and Administration, with guidance from the staffing structure review in some instances. It should be noted that TEC, with the assistance of the Human Resources Division, is running a two-year project to assist COs when conducting organizational alignment reviews, optimizing organizational structures and identifying opportunities for long-term capabilities and talent solutions. ***Roles in ICT projects*** – In most of the sampled COs, the IT unit was assigned full responsibility for the ICT functions; however, in a few instances, critical software/IT-enabled project development and maintenance activities were not visible or were managed outside the IT unit. Only one of the sampled COs had established a technical advisory group to provide guidance and recommendations on IT initiatives. ***Functional responsibilities*** – In some instances, the IT unit was responsible for building maintenance tasks, such as electrical infrastructure, that are normally the responsibility of the administration function. Five of the sampled IT units had at least one assigned electrician, with one CO having an entire "Electricity Unit" within IT. ***Staffing levels and skills*** – Criteria at the corporate or regional level to guide CO management in determining the IT units staffing and skill levels were not consistently applied and could be strengthened, to consider the number of users and IT solutions, infrastructure, number of field offices, and ICT services to be provided to other United Nations agencies. These factors should be considered to ensure the number, skills and level of competency of ICT staff is commensurate with the expected level of service and support. In the majority of cases, COs based staffing levels and skills on the availability of funds. The ICT staff to user ratio varied significantly from office to office, from 1:3 to as much as 1:62. While the average ratio of users per ICT staff was 1:8, that number jumped to 1:25 when excluding radio operators. ***Training*** – Rapidly changing technologies, and the introduction of new applications and services, heighten the criticality of keeping ICT staff skills up to date. The ICT budget of 11 of the 18 COs reviewed made no provision for the learning and development of ICT staff. ICT staff highlighted the need for more training on subjects ranging from SCOPE, digital mobile radio, IT emergency management and cloud technology. Underlying causes: IT structures recommended in corporate guidelines have not been finalized or officially adopted. There are inconsistent reporting lines for heads of IT. Development of IT systems to fill in corporate information gaps without a robust framework for oversight and control. Absence of a corporate policy, guidelines and criteria to determine the number, skills and competencies of ICT staff in COs. Lack of a talent acquisition strategy for ICT units. Skills and capacities of ICT staff are not periodically assessed to identify gaps and develop learning and development plans.	TEC will: (i) Update, finalize and publish the 2015 Field IT Governance and Management Framework, clearly establishing staffing structure models to guide CO managers, including the minimum recommended numbers of ICT staff and/or respective levels of skills, competencies and capabilities; (ii) Ensure that the RITOs liaise with COs and see that ICT activities are consolidated and monitored under the leadership of the CO's ICT function; (iii) Liaise with HR and ensure a consistent structure for the Performance and Competency Enhancement assessment of all heads of IT with the deputy country director and country director as First Reporting Officer and Second Level Reviewer, and the RITO as mandatory Functional Reviewer; and (iv) In coordination with the Management Services Division (RMM), remind COs that electricians should report and be managed under the functional responsibility of administration and not ICT

Line of enquiry 2: Is planning for ICT resources and their management adequate to ensure users are provided with the ICT systems and resources to perform their duties in the most efficient way?

The audit assessed the extent of development and purchase of IT solutions outside of TEC's corporate portfolio and the risks presented by this shadow IT. The audit also looked at how ICT assets were being managed from procurement to disposal. ICT work plans with links to the CO risk register and budgets were prepared on an annual basis and regularly monitored. ICT services provided by third parties and purchased software were mainly under corporate long-term agreements (LTAs) or otherwise covered by a service level agreement or maintenance agreement with the vendor. Sampled COs were using GEMS corporate tool, with some having piloted and adopted GEMS Mobile, thereby simplifying the physical inventory count. Inputs into GEMS were restricted to IT and administration staff in the CO with no access to staff in the sub-offices. Generally, there was coordination between ICT and administration staff, with monthly reconciliation activities. Import sanctions and delays in the clearance of ICT equipment by local authorities continue to impact project aimed at replacement of old ICT equipment. Some of the issues noted for ICT staff capacity and training have been incorporated under observation two.

Observation 3

Planning and managing the delivery and maintenance of local IT solutions

The Governance and Management Framework for Field IT established the roles, responsibilities and basic expectations for field IT software solutions development. WFP was in the process of developing a *freedom in a framework* approach, allowing for greater flexibility in the development and acquisition of IT solutions outside the direct control of TEC to fulfil business requirements not serviced by WFP corporate systems.

Nine of the 18 COs sampled had developed local IT solutions, including one CO that had locally developed 19 solutions. Certain weaknesses in the development of local information systems included:

- Lack of communication and coordination between IT and business units for the acquisition or development of IT solutions, and with TEC to ensure systems/services are not already available to fulfil the demands of the CO;
- Insufficient consideration of the capacity and readiness in the CO for digital transformation, or assessment of additional resources required for development and maintenance of the solutions (see under observation 1);
- Lack of robust systems development life-cycle (SDLC) practices in planning and managing local initiatives including the formulation of business cases, project plans, allocation of funding, release and change management procedures, business owners, etc.;
- Lack of supervision and segregation of duties between development, change management and user acceptance testing; and,
- Weak user access management and access monitoring controls and lack of monitoring by IT units to ensure compliance with good practices and established standards for change control and back-up procedures.

Underlying causes: The Governance and Management Framework for Field IT has not been reviewed to assess its effective implementation or continued relevance; *freedom in a framework* guidelines have not been formally adopted into policy or disseminated; low level of maturity of SDLC processes for the field; absence of practical SOPs for the development and acquisition of local IT solutions; lack of enforcement tools at the regional level and WFP's decentralized management models.

Agreed actions [Medium priority**]**

TEC will:

(i) Review and update the 2015 Governance and Management Framework for Field IT, and finalize and disseminate guidelines to allow for greater flexibility in the development, acquisition and maintenance of IT solutions outside the direct control of TEC, to fulfil business requirements not serviced by WFP corporate information system; and,

(ii) Through the RITOs, establish monitoring mechanisms to ensure SDLC policies and best practices are adhered to by COs when developing IT solutions.

Observation 4

Management of ICT assets

Administration has the ultimate oversight over WFP's inventory. However, the management of IT assets has, for practical purposes, been largely delegated to the IT function. The audit noted weaknesses which contribute to decreasing the performance and utility of IT assets and increase the exposure to cyber security threats and vulnerabilities.

IT asset inventory management[5] – There were weaknesses in the maintenance of accurate, complete and reliable inventory records in five of the six COs visited by the audit. Locally developed IT solutions were not always registered into WFP's IT assets inventory system (GLASS). Asset management controls in sub-offices were noted to be particularly weak due to the absence of asset management focal points or inventory clerks and robust processes to ensure asset transfers were communicated and recorded.

IT asset life-cycle management – Five of the 18 COs sampled had developed SOPs for the management of IT assets, with varying degrees of completeness. Due to budget constraints, it was common for old and obsolete IT assets to be used past their official expiry date. Eight of the COs sampled did not maintain a list or monitor out-of-warranty IT assets. Procedures and practices to cleanse data from IT equipment prior to its disposal were not standardized. In addition, there were write-offs of old or obsolete IT equipment pending approval in most of the COs visited by the audit.

We noted the Management Services Division (RMM) was in the process of finalizing an Executive Circular on Responsible Asset Management at the time of the audit, addressing some of the issues presented above from a policy perspective.

Underlying causes: Lack of adherence by COs to existing IT asset management policies and best practices. Outdated guidance covering procedures and responsibilities for the acquisition, transfer, monitoring and disposal of ICT assets; lack of detailed and up-to-date guidelines on the proper and timely disposal of obsolete, damaged and unusable ICT equipment. Cumbersome/manual asset management processes coupled with the lack of capacity of some COs. Asset management function and processes at CO level lack prioritization. Limited capacity of CO asset focal points, including knowledge of GEMS functionalities.

Agreed actions [Medium priority**]**

1. RMM, in coordination with TEC, will finalize and issue to COs the Responsible Asset Management Executive Circular covering all the responsibilities for the acquisition, transfer, monitoring and disposal of ICT assets.

2. TEC will:

(i) Work with RMM in the design of oversight monitoring controls and automation, to ensure COs are adhering to IT asset management policies and best practices, and to ensure old and obsolete IT equipment is disposed of on a timely and secure basis.

(ii) Provide COs with supplementary guidelines covering all the procedures for the acquisition, transfer, monitoring and disposal of ICT assets not already covered under the Responsible Asset Management Executive Circular.

[5] Reference to the audit of asset management

Line of enquiry 3: Are effective logical and physical security mechanisms in place to prevent unauthorized access to programs, data and computer installations, and detect any violation of security?

The audit looked at whether responsibility for the administration of security access to ICT systems and data was clearly defined, and controls in place, to ensure compliance with corporate cybersecurity policies. It reviewed the assignment and restrictions in accessing WFP's network, and the degree of proactive monitoring to identify unauthorised access to information systems and data. In the case of the corporate enterprise resource planning platform WINGS, the audit reviewed the extent of non-standard requests for access and controls to ensure compliance with corporate segregation of duties standards.

Responsibility for the administration of security access to corporate systems and data was assigned to the IT unit. All surveyed COs referred to the "WFP Corporate Information and IT Security Policy" as their guide for matters on IT security. We noted that access rights to WFP's network were granted and revoked following set procedures. Regular monitoring ensured that workstations not compliant with WFP security configuration standards were identified and their number kept to a minimum. Non-standard requests for access rights to WINGS, including Officer-in-Charge authorization, followed the prescribed assessment and approval procedure. Access to the data centres located in COs was generally in conformity with security standards, with entry restricted to designated IT staff by means of magnetic swipe cards. The centres were provided with smoke detectors and fire extinguishers, and in most cases, there was CCTV monitoring.

Observation 5	**Agreed actions [**Medium priority**]**
Administration of security access, use of personal devices and segregation of duties in WINGS ***Access management responsibilities and rights*** – Only one of the units sampled by the audit had a documented matrix of responsibilities and levels of access to the various components of the CO's system, including servers and workstation administration, network drives, applications, databases and peripheral devices. Centralized access management to key systems (i.e. WINGS, SCOPE, etc.) partially mitigated the risk of unauthorized assess. ***Personal devices*** – WFP staff could bring personal mobile devices such as smartphones, laptops and tablets to work, posing potential security and privacy challenges. We noted there was no documented Bring Your Own Device (BYOD) security policy. To mitigate potential risks, IT units created separate restricted guest networks for private and visitor access. In addition, the corporate firewall isolated access to the corporate systems and helped in controlling the usage of bandwidth. However, the increase in the use of personal devices require a policy to provide guidance to users and IT staff. ***SAP (WINGS) GRC: Compliance with global segregation of duty (SOD) standards and implementation of mitigating controls*** – To control user access to WINGS (WFP's enterprise resource planning systems), TEC, in coordination with key business owners, has developed SOD matrices by business function, identifying patterns and making recommendations to reduce the number of non-standard assignments. At the CO level, there was insufficient awareness of the matrices to allow managers and role-owners identify SOD risks when requests for access were submitted and granted. Underlying causes: Absence of monitoring and enforcement mechanisms to ensure access levels and responsibilities of IT staff are documented; absence of a corporate BYOD policy; governance framework to ensure compliance with global SOD standards have been defined but were yet fully functioning; better communication is needed between TEC and business units when implementing changes to corporate tools and applications.	TEC will: (i) In coordination with the RITOs, implement monitoring and enforcement mechanisms to ensure CO IT units maintain an up-to-date administration and security access approved matrix, and allow for compensating controls when the COs are not able to comply with recommended guidelines; and, (ii) Develop and implement a BYOD policy for personal devices, documenting user permissions and responsibilities.

Line of enquiry 4: Are users provided with continued IT services, support, documentation and training to enable them to use the systems correctly and effectively?

The audit reviewed the effectiveness of ICT procedures to deal with instances of significant operational failure, the management of user requests for ICT services and reporting of incidents, whether users were provided with the necessary training on IT security awareness and the use of corporate applications. In the management of continuity, the audit considered four main elements that contribute to ensure the availability of business-critical systems and information: stable connectivity, and, depending on the extent of a disruption in the ICT service, the availability of back-ups and a recently tested IT Disaster Recovery Plan that is integrated within the CO's Business Continuity Plan and/or emergency preparedness response package.

The IT units considered the corporate IT Operations Manual adequate for guidance with only one of the sampled COs developing a standard operating procedure in support. The COs did not report any major operational failures that resulted in systems being unavailable for an extended period, or to loss of data. System failures were exceptional and resulted in minimum downtime. One exception involved the intermittent rebooting of IP phones, over a period of four months, affecting both the CO and RB as well as other United Nations agencies in the area. The IT unit immediately took up the matter with the service provider, a United Nations agency, and the problem was eventually resolved. TEC had a team dedicated to monitor connectivity in the field and to provide support. Connectivity issues were limited to specific geographical areas and are discussed below. Most COs were performing back-ups in line with corporate requirements, with weaknesses noted mostly at the sub-office levels. However, guidelines need to be updated to reflect WFP's increasing use of cloud services.

In addition to the corporate IT Service Desk, users in 14 of the sampled offices had a local help desk management system to register their requests for assistance and report ICT-related incidents. Back-up cycles were in line with corporate guidelines.

Observation 6

Manage continuity

Ensuring reliable and continuous communications and availability of data and preparing for contingent scenarios are essential operational requirements at WFP. In this regard, the audit had the following observations:

Connectivity – TEC policy dictates COs route corporate application traffic (i.e. WINGS, LESS, SCOPE, etc.) via VSAT while local internet service providers (ISPs) should be used for email and non-core requirements. While most COs reported adequate ISP connectivity, these were not always available, especially for COs operating in the West and Central Africa region, increasing the load on the VSAT bandwidth. Old and obsolete equipment further deteriorated communications in some COs. Deep field locations including sub-offices and warehouses were especially susceptible to a marked deterioration in connectivity, impacting their ability to process finance and supply chain transactions and manage beneficiary data.

TEC performed assessments and provided capacity reports with analysis and recommendations to country offices on bandwidth management. However, continued connectivity issues indicate these reports have not been heeded and a strategic approach is needed to achieve sustainable connectivity solutions. We noted TEC is in the process of optimizing WAN since 2018 and is compiling a Request for Proposal for satellite communication services to improve connectivity at the field level.

Agreed actions [High priority]

TEC will:

(i) Bring to completion its ongoing initiatives, including the optimization of WAN and satellite communication services;

(ii) Develop and provide COs disaster recovery plan templates, ensuring these capture all critical aspects of an IT disaster recovery plan, including provision for the ICT function to operate from an alternative site and for regular testing; and,

(iii) In coordination with the Emergency Preparedness and Support Response and Enterprise Risk Management Divisions, review the adequacy of current BCP policies, ensuring potential business continuity risks are thoroughly assessed, supported by business impact analysis, and aligned to risk management practices.

Observation 6	Agreed actions [High priority]
IT disaster recovery and business continuity planning – Disaster recovery plans were not consistently updated, made provision for testing or identified an alternative site. While 11 of the 18 COs sampled had developed a business continuity plan (BCP), we noted five of these had not been updated for two years or more and did not reflect changes in the IT system environment, and only one had been tested. Another three had a scope limited to the recovery of IT systems without addressing the wider aspects of business continuity. There was a low level of awareness among heads of business units of continuity planning, with most of them not sure what was expected of them in the event of a serious incident or disaster. ***Governance*** – Under the present corporate guidelines, it was no longer mandatory for COs to have a BCP as long as detailed continuity guidelines were captured in their emergency preparedness and response package (EPRP). While three COs followed this approach, the EPRPs developed did not cover the entire scope of business continuity or potential risks normally addressed by a BCP. Underlying causes: Lack of a strategic approach to address connectivity issues; absence of an IT disaster recovery plan template to ensure completeness and facilitate implementation; EPRP is not an adequate vehicle to address business continuity objectives or risks.	

Annex A – Summary of observations

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

	High priority observation	WFP's Internal Control Framework	WFP's Enterprise Risk Management Framework	WFP's Internal Audit Universe	Implementation Lead	Due date
6	Manage continuity	Control Activities	ICT	Business Continuity Management	TEC	31.12.2019
	Medium priority observations					
1	Governance and strategic planning	Control Enviroment	ICT	ICT governance and strategic planning	TEC Chair of MISSC RMR	31.12.2019 30.06.2019 31.03.2020
2	Structure, staffing and responsibilities of the ICT function	Control Enviroment	ICT	ICT governance and strategic planning	TEC	31.12.2019
3	Planning and managing the delivery and maintenance of local IT solutions	Control Enviroment	ICT	Selection/development and implementation of IT projects	TEC	30.10.2019
4	Management of ICT assets	Control Activities	Assets	Asset management	RMM TEC	30.09.2019 30.09.2019
5	Administration of security access, use of personal devices and segregation of duties in WINGS	Control Activities	ICT	Security administration/controls over core application systems	TEC	31.03.2020

Annex B – Definitions of audit terms: ratings & priority

1 Rating system

1. 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 Categorization of audit observations and priority of agreed actions

2.1 Priority

2. Audit observations are categorized according to the priority of the agreed actions, which serves 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.

3. 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.

4. 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.[6]

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

2.2 Categorization by WFP's Internal Control Framework (ICF)

6. WFP's ICF follows principles from the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Integrated ICF, adapted to meet WFP's operational environment and structure. WFP defines internal control as: "a process, effected by WFP's Executive Board, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, compliance."[7] WFP recognizes five interrelated components (ICF components) of internal control, all of which need to be in place and integrated for them to be effective across the above three areas of internal control objectives.

Table B.3: Interrelated Components of Internal Control recognized by WFP

1	Control Environment	The control environment sets the tone of the organization and shapes personnel's understanding of internal control
2	Risk Assessment	Identifies and analyses risks to the achievement of WFP's objectives through a dynamic and iterative process.
3	Control Activities	Ensure that necessary actions are taken to address risks to the achievement of WFP's objectives.
4	Information and Communication	Allows pertinent information on WFP's activities to be identified, captured and communicated in a form and timeframe that enables people to carry out their internal control responsibilities.
5	Monitoring Activities	Enable internal control systems to be monitored to assess the systems' performance over time and to ensure that internal control continues to operate effectively.

2.3 Categorization by WFP's Enterprise Risk Management Framework (ERM)

7. WFP has developed a risk categorization framework to assist management at all levels as well as to improve risk analysis. The framework enables offices and operations to identify risks using a common language across WFP. Risks are classified into four primary categories: strategic, operational, fiduciary and financial. Reputational risk is defined as a consequential risk whereby risks occurring in any category could have a negative impact on WFP's reputation. Within these four categories, 15 risk areas covering the scope of WFP's enterprise risk management have been defined.

Table B.4: WFP's new risk categorization recognizes 4 risk categories and 15 types of risk

1	Strategic	1.1 Programme risks, 1.2 External relationship risks, 1.3 Contextual risks, 1.4 Failure to innovate/adjust business model

[6] An audit observation of high risk to the audited entity may be of low risk to WFP as a whole; conversely, an observation of critical importance to WFP may have a low impact on a specific entity, but have a high impact globally.

[7] OED 2015/016: paragraph 7.

2	Operational	2.1 Beneficiary health, safety & security risks, 2.2 Staff health, safety & security risks, 2.3 Partner & vendor risks, 2.4 Asset risks, 2.5 ICT failure/disruption/attack, 2.6 Business process risks, 2.7 Governance & oversight breakdown
3	Fiduciary	3.1 Breach of obligations, 3.2 Fraud & corruption
4	Financial	4.1 Adverse price/cost change, 4.2 Adverse asset outcome

2.4 Categorization by WFP's Audit Universe

8. WFP's audit universe[8] covers organizational entities and processes. Mapping audit observations to themes and process areas of WFP's audit universe helps prioritize thematic audits.

Table B.5: WFP's 2018 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	Programme	(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	Operations	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 & 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; Monitoring and Evaluation (M&E) framework; Gender; Protection; Environmental management.

[8] A separate universe exists for information technology with 60 entities, processes and applications.

5. Monitoring the implementation of agreed actions

9. 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 timeframe to manage and mitigate the associated risks identified, thereby contributing to the improvement of WFP's operations.

Annex C – Acronyms

BCP	business continuity plan
BYOD	Bring Your Own Device
EPRP	emergency preparedness response package
GEMS	Global Equipment Management System
ICT	information and communications technology
IT	Information technology
KPI	key performance indicator
MISSC	Management Information Systems Steering Committee
RITO	Regional Information Technology Officer
RMR	Enterprise Risk Management Division
SAP	An enterprise resource planning software by German developer, SAP AG
SDLC	Systems Development Lifecycle
SOP	Standard Operating Procedure
TEC	Technology Division
WFP	World Food Programme
WINGS	WFP Information Network and Global System, WFP's ERP system