Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2020/047

Audit of information technology continuity at the Office of the United Nations High Commissioner for Refugees

There was a need to establish a regulatory framework and plan for information technology continuity, perform business impact analysis, establish disaster recovery arrangements for critical systems and explore viable solutions to store backed-up field data

1 December 2020
Assignment No. AR2020-166-02

Audit of information technology continuity at the Office of the United Nations High Commissioner for Refugees

EXECUTIVE SUMMARY

The Office of Internal Oversight Services (OIOS) conducted an audit of information technology (IT) continuity at the Office of the United Nations High Commissioner for Refugees (UNHCR). The objective of the audit was to assess whether effective measures were in place for information technology continuity in UNHCR and to ensure that interruptions to IT systems do not disrupt programme delivery. The audit covered: (a) framework for IT continuity; (b) identification of IT assets and risks related to their unavailability; (c) mapping of critical business processes to support IT assets; (d) establishment of contingency strategies; and (e) regular review and update of the IT continuity plan.

Despite disruption by Covid-19, UNHCR adapted efficiently and seamlessly to digital solutions to ensure that it remained operational. The Covid-19 crisis accelerated the digitalization of the operational framework in UNHCR with increased use of teleworking and video conferencing systems, and the Division of Information Systems and Telecommunications played a key role in ensuring the continuity of IT services during the crisis. However, improvement was needed in some areas.

OIOS made four recommendations. To address issues identified in the audit, UNHCR needed to:

- Establish an IT continuity framework, IT continuity plan and a process to regularly update the IT continuity plan in line with changing business needs;
- Undertake a comprehensive business impact analysis by documenting: (a) critical business functions and related IT systems; (b) the maximum allowable outage for critical business functions, recovery time and recovery point objectives; (c) the operational and financial impacts of disruption to critical business functions; and (d) business continuity plans;
- Ensure that disaster recovery arrangements are in place for all applications and systems that support critical business processes; and
- Explore viable solutions including cloud services for securely storing a copy of the backed-up data for its field offices.

UNHCR accepted the recommendations and has initiated action to implement them.

CONTENTS

Audit of information technology continuity at the Office of the United Nations High Commissioner for Refugees

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of information technology (IT) continuity at the Office of United Nations High Commissioner for Refugees (UNHCR).

2. Information system resources are fundamental to an organization, and it is critical that services provided by these systems operate effectively without excessive interruption. Information systems are vulnerable to a variety of disruptions ranging from mild (such as power outage, disk drive failure) to severe (such as natural disasters and fire). Vulnerability may be minimized or eliminated through management, operational, or technical controls as part of the organization's resiliency efforts. IT continuity planning is the process that ensures continuous operations of business applications and supporting IT systems. According to the National Institute of Standards and Technology (NIST)[1], information system contingency planning refers to a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, operations, and data after a disruption.

3. IT disaster recovery is one of the core elements of the Organizational Resilience Management System of the United Nations Secretariat, approved by the General Assembly in resolution A/RES/67/254. Recent events such as the ongoing Covid-19 outbreak presented serious challenges for business continuity as UNHCR needed to be equipped to handle technology risks with most staff being forced to work remotely. During pandemic based scenarios, effective IT systems are crucial for business continuity.

4. The Disaster Recovery Planning - United Nations Secretariat Information and Communication Technology (ICT) Technical Procedure issued in July 2014 establishes requirements to ensure high availability of United Nations ICT resources and data. The purpose of the Technical Procedure is to prescribe the development and implementation of disaster recovery plans and procedures that can provide a prompt and effective continuation of critical ICT services in event of service disruption.

5. Comments provided by UNHCR are incorporated in italics.

II. AUDIT OBJECTIVE, SCOPE AND METHODOLOGY

6. The objective of the audit was to assess whether effective measures were in place for IT continuity in UNHCR and ensure that interruptions to IT systems do not disrupt programme delivery.

7. This audit was included in the 2020 risk-based work plan of OIOS because of the inherent risk of interruption to business processes caused by failure of IT systems, which could adversely affect delivery of UNHCR's mandate.

8. OIOS conducted this audit in March and April 2020 and covered current controls in place over continuity of IT systems in use at the time of audit. Based on an activity-level risk assessment, the audit covered the following higher and medium risks areas: (a) framework for IT continuity; (b) identification of IT assets and risks related to their unavailability; (c) mapping of critical business processes to support IT assets; (d) establishment of contingency strategies; and (e) regular review and update of the IT continuity plan.

[1] United States Federal Government agency that promotes innovation and industrial competitiveness by advancing measurement science, standards, and technology.

9. The audit methodology included: (a) interviews with key personnel; (b) review of relevant documentation; (c) analytical review of data from UNHCR IT systems; and (d) sample testing of controls. OIOS also reviewed: arrangements for teleworking for UNHCR staff members; data from the Global Service Desk for the period 15 March to 15 April 2020; and situation reports from Regional Bureaux on IT challenges faced in programme implementation. Additionally, although OIOS initially planned to travel to Amman, Jordan to review IT continuity arrangements for the Regional Bureau of the Middle East and North Africa (MENA), due to the travel ban and lockdown, relevant information was obtained through virtual interactions.

10. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

III. AUDIT RESULTS

A. Regulatory framework and planning for IT continuity

DIST successfully ensured the continuation of IT services during the pandemic

11. Despite disruption by Covid-19, UNHCR adapted efficiently and seamlessly to digital solutions to ensure that the Organization remained operational. The unprecedented Covid-19 crisis accelerated the digitalization of the operational framework in UNHCR, with increased use of teleworking and video conferencing systems. The Division of Information Systems and Telecommunications (DIST) played a key role in ensuring the continuity of IT services during the crisis and its tools continued to facilitate UNHCR's work during the pandemic.

12. DIST issued Global IT Guidance for Teleworking which provides a checklist, essential resources and guidance for working remotely. In a survey on teleworking experiences at the Headquarters in Geneva, about 550 respondents of 672 (over 80 per cent) confirmed that the overall experience in carrying out work duties remotely was positive. This included the IT equipment they used, the cloud-based tools to access work files, and the use of online tools for communication and meetings.

13. The number of requests for virtual private network services to access the files from remote locations increased from 92 in February 2020 (before the lockdown) to 533 at the end of March 2020. UNHCR's Global Service Desk data showed that of the 14,300 IT incidents recorded between mid-March to mid-April 2020, only 215 (or 1.5 per cent) were critical and high priority incidents. Of these, all but five were resolved, which indicated that IT services were delivered without major interruptions. There were also increased demands for IT support from Representations for facilitating community outreach and legal counselling using telecommunications and social media. Situation reports from Regional Bureaux confirmed that additional hotline support was provided to families in need. Consideration was also being given to carrying out refugee status determination interviews remotely on a pilot basis, along with remote registration and document renewal. The audit however, identified areas for improvement in IT continuity, as outlined in the report.

There was a need for a regulatory framework for IT continuity and have an IT continuity plan

14. DIST has the responsibility to develop and maintain ICT policies, standards and guidelines designed for the establishment of controls for addressing identified ICT risks. NIST also specifies that to be effective and to ensure that staff fully understand the organization's contingency planning requirements, the IT continuity plan must be based on a clearly defined policy.

15. Whilst DIST had identified high and medium-risk areas pertaining to IT continuity, such as failure of IT infrastructure, deficient data storage, inadequate backup and recovery processes, UNHCR did not have a formal policy framework and an IT continuity plan for continuation of critical IT services following a disruptive event. Such a framework, as recommended by NIST, should specify key elements such as roles and responsibilities, scope, resource and training requirements, exercise and testing schedules, a planned maintenance schedule, and minimum frequency of backups and storage of backup media. The IT continuity plan should provide the steps needed to recover all or part of designated information systems at an existing or new location in an emergency. The plan should also include key information such as roles and responsibilities, inventory, procedures for recovery, and systems testing. The IT contingency plan needs to be kept up to date.

16. Moreover, UNHCR's newly established decentralized and regionalized structure, whereby Regional Bureaux and Representations are expected to operate autonomously and have significant authority delegated to them, has implications for IT continuity planning. This is because, even prior to decentralization, Representations (particularly large ones) had established local IT infrastructure and developed software applications that were not supported centrally by DIST. This issue is discussed later in the report. The increased delegation of authority, therefore, could result in further proliferation of local IT infrastructure and applications outside the remit of DIST's control, and may have implications for effective IT continuity in UNHCR.

17. Therefore, arrangements in place for ensuring IT continuity require reassessment in a decentralized and regionalized UNHCR to improve clarity, such as: (i) how DIST would deliver on its accountabilities for IT continuity in a decentralized and regionalized context; (ii) how DIST would achieve the right balance between having a role of global oversight of IT matters, including IT continuity and the empowered and autonomous Regional Bureaux/Representations; and (iii) whether DIST has the tools and authority needed to deliver assurance of IT continuity to UNHCR globally. For critical matters such as IT continuity, there needs to be institutional coherence and clarity of approaches.

18. Without a formal framework/policy document and an updated IT continuity plan, there is a risk that disruptions to IT services could trigger inconsistent actions which could adversely affect decision making in UNHCR and interrupt programme delivery.

(1) The UNHCR Division of Information Systems and Telecommunications (DIST) should establish: (a) a framework and an information technology continuity plan which takes into consideration DIST's accountabilities for information technology continuity in a decentralized and regionalized context; and (b) a process to regularly update the information technology continuity plan in line with changing business needs.

UNHCR accepted recommendation 1 and stated that DIST would establish an IT continuity framework by mid-2021. The framework would take into consideration the current context, would be aligned with the business needs and updated as required. Recommendation 1 remains open pending receipt of a framework setting out DIST's responsibilities and accountabilities for IT continuity, the IT continuity plan and the process to update it in accordance with changing business needs.

<u>Critical business processes needed to be mapped to the supporting IT assets and business impact analysis performed</u>

19. The United Nations Secretariat ICT Technical Procedure has defined business impact analysis (BIA) as an analysis of an information system's requirements, functions, and interdependencies used to characterize system disaster recovery requirements and priorities in the event of a significant disruption. The purpose of BIA is to correlate the system with critical business processes and services provided, and

based on that information, characterize the consequences of a disruption. The BIA helps identify and prioritize information systems and components critical to supporting the organization's business processes.

20. A business process is considered critical, if its interruption will compromise one or more of the organization's critical functions. If the process cannot be recovered within a defined timeframe, this could result in loss of life, or the inability to provide the affected critical function(s). A critical application is defined as an IT system that is essential to perform a critical business process.

21. For a business continuity plan (BCP) to be effective and successful, business owners (such as UNHCR Divisions, Regional Bureaux and Representations) with the support of the IT service provider (DIST) must establish the critical information resources that support key business processes by undertaking a BIA. The BCP should be periodically reviewed to confirm its suitability, particularly when there are changes in technology, processes and/or the external environment. The Controller and Director, Division of Financial and Administrative Management (DFAM), is the designated focal point for the Organizational Resilience Management System in UNHCR of which IT disaster recovery is a core element.

22. UNHCR developed BCPs for Headquarters and field offices to respond to the ongoing Covid-19 pandemic. These listed the critical functions for each Division, responsible primary and backup staff members, locations from where the process could be performed, critical vendors and recovery strategies. These were positive initial steps, but the BCPs reviewed did not include all key elements required in terms of the United Nations Technical Procedure. For example, they did not:

- Include BIA to determine which processes are critical for business continuity;
- Identify and prioritize information systems and components critical to supporting the organization's business processes; and
- Correlate the information systems with critical business processes and services provided, and based on that information, characterize the consequences of a disruption, and prioritize the recovery time objectives and the recovery point objectives.

23. Therefore, from an IT perspective, while critical business processes had been identified, corresponding actions had not been taken in developing a comprehensive BIA to identify critical IT systems underlying and supporting critical business processes. For example, while the Representations in the MENA Regional Bureaux had formulated BCPs for their operations that included information on processes, roles and responsibilities and had an overview of IT systems, the BCPs did not include mitigation measures in case of a disruptive event on a critical business process nor did they specify their recovery time[2] and recovery point objectives.

24. In 2016, to support the Headquarters Divisions, DIST performed an initial BIA, which was limited in scope and documented critical corporate systems and related business processes. This exercise identified the downtime reflecting the maximum time that UNHCR could tolerate while still maintaining its operations following a disruptive event. DIST explained that this information could not be used to develop a UNHCR comprehensive global disaster recovery plan due to the lack of available resources and also due to the non-inclusion of the systems used by the Representations.

25. The overall gaps in the BCP/BIA process can be illustrated with reference to cash-based intervention (CBI) activities, a key business process, particularly in the MENA region. UNHCR spent $1.72 billion from 2017 to 2019 on CBI activities or 20 per cent of the total operational expenditure of $8

[2] Recovery Point Objective (RPO): The point in time to which data must be recovered after a disruption has occurred. Recovery Time Objective (RTO): The period within which minimum levels of services and/or products and the supporting systems, applications or functions must be recovered after a disruption has occurred.

billion. While the Representation in Greece used CashAssist, the corporate application to facilitate CBI, several Representations in MENA used different non-corporate IT solutions to implement and manage CBI activities amounting to $1.5 billion. Whilst UNHCR Representations identified risks relating to policies and procedures, fraud, mismanagement and budgets, and the related mitigation measures in the corporate risk register, they did not specifically identify in the BCP or in the corporate risk register the local IT systems that supported critical CBI processes and the potential disruptions to the operations if the enabling IT systems were not available.

26. While DIST is responsible for all corporate systems, they did not support the non-corporate intermediary IT systems used by the Representations. In the BCPs reviewed, OIOS did not find that Representations had assessed the criticality of these systems including the length of time they could continue their operations if these non-corporate IT solutions were unavailable, as the recovery time and recovery point objectives had not been established. Risks to UNHCR Representations were exacerbated because of lack of capacity of these systems to meet the changing business needs, absence of vendor support and technology obsolescence, which could affect their continued availability to support the business processes.

27. With the lapse of time since the last BIA study in 2016 and the major structural changes impacting the Headquarters Divisions, Regional Bureaux and Representations, UNHCR needs to conduct a new and comprehensive BIA to identify and document the correlation between IT systems and the critical business processes at Headquarters, Regional Bureaux and at the Representations and describe the consequences of a disruptive event. The results of this exercise should form the basis for updating the BCPs.

(2) The Deputy High Commissioner should task the Division of Financial and Administrative Management and the Division of Information Systems and Telecommunications to work together to undertake a comprehensive business impact analysis by documenting: (a) critical business functions and the related information technology systems that support them, together with risks and resource dependencies; (b) the maximum allowable outage for critical business functions, recovery time and recovery point objectives for the supporting information systems; (c) the operational and financial impacts of disruption to critical business functions; and (d) business continuity plans based on the results of the business impact analysis.

UNHCR accepted recommendation 2 and stated that UNHCR had already prepared a BCP as part of a document called UNHCR Crisis Management Team (Headquarters Geneva) Playbook, which was at an advanced stage of completion and included a list of critical business functions. DFAM would further enhance this document to address the recommendation with respect to recovery time and impact, and to reflect the experience gathered during the COVID crisis. The document would constitute the basis for DIST to identify and analyze the necessary supporting IT systems and complete the BIA. Based on the results of the BIA, the Playbook would be updated to reflect the support needed for global IT systems during a crisis. Furthermore, field offices would be advised to include provisions for ensuring continuity of their critical local IT systems in their local BCPs. The recommendation should be implemented by mid-2021. Recommendation 2 remains open pending receipt of the BIA detailing the: critical business functions; IT systems that support them; maximum allowable outage times; recovery times; the impact on UNHCR in case of a disruptive event; and BCPs based on business impact analysis.

B. Disaster recovery and backup arrangements

There was a need to ensure disaster recovery arrangements for all critical IT systems

28. The UNHCR Operational Guidelines on ICT Security specify that DIST in close coordination with responsible UNHCR managers will ensure that adequate and reliable backup and recovery procedures are in place, tested, stored, and monitored for UNHCR's ICT systems.

29. DIST works closely with Divisions and Regional Bureaux to design, develop and support UNHCR's corporate Business Applications. UNHCR applications such as MSRP[3], Focus[4], PRIMES[5], and the intranet are considered critical applications. MSRP, intranet and Focus are hosted by a United Nations Agency, and in the agreement with them, once a disaster is officially declared, the disaster recovery environment for MSRP production would be made available within 24 hours with a maximum of 4 hours data loss, and for Focus, the corresponding times were 120 hours and 24 hours respectively. Similar arrangements were in place for the UNHCR intranet.

30. PRIMES is hosted at a private data centre, where a managed services provider backed up the data every week, with backup media held at the UNHCR office in Geneva. With assured redundancy[6] of infrastructure at this data centre, continued availability of these applications has been ensured. For PRIMES, UNHCR has specified the point in time to which data must be recovered after a disruptive event is one day (or one day of data loss would be acceptable). However, no assessment had been made of the maximum time UNHCR could continue with its protection programmes without these systems being available (or the period of time within which minimum levels of services and/or products and the supporting systems must be recovered after a disruption). Lastly, should the data centre site itself be not available or destroyed, there would be no possibility for UNHCR to access the applications as the contract with the data centre did not cover the disaster recovery arrangements.

(3) The UNHCR Division of Information Systems and Telecommunications should ensure that disaster recovery arrangements are in place for all applications and systems that support critical business processes.

UNHCR accepted recommendation 3 and stated that depending on funding availability, the applications and systems supporting critical processes would be included in disaster recovery arrangements by the end of 2021. Recommendation 3 remains open pending receipt of evidence confirming that the disaster recovery arrangements are in place for all critical systems.

Backed-up data of field locations should be securely stored

31. NIST specifies that system data should be backed up regularly. Policies should specify the minimum frequency and scope of backups (daily or weekly, incremental or full) based on data criticality and the frequency that new information is introduced. Data backup policies should designate the location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite. Also, it is good business practice to store backed-up data offsite.

32. DIST has issued Office Infrastructure Server (OIS) policies and procedures for the backup, restoration and execution of local off-site archiving of data. For instance, the backup covered the short-

[3] Managing for Systems, Resources and People, the UNHCR enterprise resource planning system.

[4] Focus is UNHCR's Results-Based Management tool.

[5] UNHCR Population Registration and Identity Management EcoSystem.

[6] Provision of duplicate, backup equipment or links that immediately take over the function of equipment or transmission lines that fail.

term protection of files against accidental deletion, overwrite or logical corruption and protection against major file and print server failure. Furthermore, it also required offsite storage of backed up data to ensure protection against theft, or destruction of the OIS server. Separate procedures were in place to back up and store data pertaining to the legacy proGres v3 data. A managed services provider was responsible for the automatic backup of the OIS data, and an IT focal point in each location was responsible to copy the backed-up data to an external storage device for safe-keeping at another geographical location.

33. DIST received a monthly feedback from field locations on the level of compliance regarding the backup performed. OIOS noted; however, that compliance levels were low. For instance, in December 2019, 288 out of the 551 field locations (52 per cent) confirmed that backups of critical systems and file drives were performed on a regular basis. In March 2020, the overall compliance level decreased and only 102 (24 per cent) out of 421 locations confirmed performance of the backups, with the decline partially attributable to the onset of the pandemic. Furthermore, regarding the offsite storage of critical backup media, documentation and other IT resources necessary for IT recovery and BCPs, only 68 (16 per cent) out of the 421 locations confirmed compliance.

34. The poor compliance levels were due to the absence of IT focal points or staff with IT expertise in Representations, with reduction in 2020 due to the pandemic as previously noted. Consequently, there was a risk of data loss and interruption to operations in case the field OIS server was damaged or stolen and should be mitigated.

(4) The UNHCR Division of Information Systems and Telecommuncations should explore viable solutions including cloud services for securely storing a copy of the backed-up data for its field offices.

UNHCR accepted recommendation 4 and stated that DIST would explore by mid-2021, the most efficient and effective solutions for securely storing a copy of the back-up data for the field offices. Recommendation 4 remains open pending receipt of evidence of secure storage of backed-up data for field offices.

IV. ACKNOWLEDGEMENT

35. OIOS wishes to express its appreciation to the management and staff of UNHCR for the assistance and cooperation extended to the auditors during this assignment.

(*Signed*) Eleanor T. Burns
Director, Internal Audit Division
Office of Internal Oversight Services

STATUS OF AUDIT RECOMMENDATIONS

Audit of information technology continuity at the Office of the United Nations High Commissioner for Refugees

Rec. no.	Recommendation	Critical[7]/ Important[8]	C/ O[9]	Actions needed to close recommendation	Implementation date[10]
1	The UNHCR Division of Information Systems and Telecommunications (DIST) should establish: (a) a framework and an information technology continuity plan which takes into consideration DIST's accountabilities for information technology continuity in a decentralized and regionalized context; and (b) a process to regularly update the information technology continuity plan in line with changing business needs.	Important	O	Receipt of a framework setting out DIST's responsibilities and accountabilities for IT continuity, the IT continuity plan and the process to update it in accordance with changing business needs.	30 June 2021
2	The Deputy High Commissioner should task the Division of Financial and Administrative Management and the Division of Information Systems and Telecommunications to work together to undertake a comprehensive business impact analysis by documenting: (a) critical business functions and the related information technology systems that support them, together with risks and resource dependencies; (b) the maximum allowable outage for critical business functions, recovery time and recovery point objectives for the supporting information systems; (c) the operational and financial impacts of disruption to critical business functions; and (d) business continuity plans based on the results of the business impact analysis.	Important	O	Receipt of the BIA detailing the: critical business functions; IT systems that support them; maximum allowable outage times; recovery times; the impact on UNHCR in case of a disruptive event; and BCPs on business impact analysis.	31 December 2021
3	The UNHCR Division of Information Systems and Telecommunications should ensure that disaster recovery arrangements are in place for all	Important	O	Receipt of evidence confirming that the disaster recovery arrangements are in place for all critical systems.	31 December 2021

[7] Critical recommendations address those risk issues that require immediate management attention. Failure to take action could have a critical or significant adverse impact on the Organization.

[8] Important recommendations address those risk issues that require timely management attention. Failure to take action could have a high or moderate adverse impact on the Organization.

[9] Please note the value C denotes closed recommendations whereas O refers to open recommendations.

[10] Date provided by UNHCR in response to recommendations.

STATUS OF AUDIT RECOMMENDATIONS

Audit of information technology continuity at the Office of the United Nations High Commissioner for Refugees

Rec. no.	Recommendation	Critical[7]/ Important[8]	C/ O[9]	Actions needed to close recommendation	Implementation date[10]
	applications and systems that support critical business processes.				
4	The UNHCR Division of Information Systems and Telecommuncations should explore viable solutions including cloud services for securely storing a copy of the backed-up data for its field offices.	Important	O	Receipt of evidence of secure storage of backed-up data for field offices.	30 June 2021

Annex II

Cost-benefit analysis of the implementation of recommendations

Audit of information technology continuity at the Office of the United Nations High Commissioner for Refugees

Recommendation	Implementation costs	Implementation benefits
1. The UNHCR Division of Information Systems and Telecommunications (DIST) should establish: (a) a framework and an information technology continuity plan which takes into consideration DIST's accountabilities for information technology continuity in a decentralized and regionalized context; and (b) a process to regularly update the information technology continuity plan in line with changing business needs.	Given that the new framework needs to consider DIST's accountabilities for IT continuity in a decentralized and regionalized context, OIOS anticipates medium to high investment, since the framework needs to be established.	A framework and continuity plan will enable the implementation of structured and consistent processes for IT continuity across the Organization. It will also ensure that staff fully understand UNHCR's contingency planning requirements.
2. The Deputy High Commissioner should task the Division of Financial and Administrative Management and the Division of Information Systems and Telecommunications to work together to undertake a comprehensive business impact analysis by documenting: (a) critical business functions and the related information technology systems that support them, together with risks and resource dependencies; (b) the maximum allowable outage for critical business functions, recovery time and recovery point objectives for the supporting information systems; (c) the operational and financial impacts of disruption to critical business functions; and (d) business continuity plans based on the results of the business impact analysis.	Medium to high investment as it will take time and effort to undertake a BIA and thereafter put together BCPs in a decentralized and regionalized UNHCR.	A BIA and up to date BCPs improve visibility of critical systems and processes used by UNHCR including at Representations as well as a systematic way of identifying related risks. Overall, UNHCR will be better equipped to handle disruptive and unforeseen events.
3. The UNHCR Division of Information Systems and Telecommunications should ensure that disaster recovery arrangements are in place for all applications and systems that support critical business processes.	Low to medium investment as disaster recovery arrangements are already in place for most critical corporate applications. However, additional costs may be incurred in some cases.	UNHCR will be better prepared to continue performing critical business processes after a disruptive event as well as the support necessary for its critical systems and applications.
4. The UNHCR Division of Information Systems and Telecommuncations should explore viable solutions including cloud services for securely storing a copy of the backed-up data for its field offices.	Low to medium investment may be incurred in some locations to securely store backed-up data.	UNHCR data will be kept safe and secure.

APPENDIX I

Management Response

APPENDIX I

Management Response

Audit of information technology continuity at the Office of the United Nations High Commissioner for Refugees

Rec. no.	Recommendation	Critical[11]/ Important[12]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	The UNHCR Division of Information Systems and Telecommunications (DIST) should establish: (a) a framework and an information technology continuity plan which takes into consideration DIST's accountabilities for information technology continuity in a decentralized and regionalized context; and (b) a process to regularly update the information technology continuity plan in line with changing business needs.	Important	Yes	Deputy Director BRMS/ DIST	Q2 2021	DIST will establish an IT Continuity framework by Q2 2021. The framework will take into consideration the current context, will be aligned with the business needs and updated as required.
2	The Deputy High Commissioner should task the Division of Financial and Administrative Management and the Division of Information Systems and Telecommunications to work together to undertake a comprehensive business impact analysis by documenting: (a) critical business functions and the related information technology systems that support them, together with risks and resource dependencies; (b) the maximum allowable outage for critical business functions, recovery time and recovery point objectives for the supporting information systems; (c) the operational and financial impacts of disruption to critical business functions; and (d) business continuity plans	Important	Yes	Deputy Director BRMS/DIST Deputy Director DFAM	Q4 2021	UNHCR has already prepared a BCP as part of a document called UNHCR Crisis Management Team (HQ Geneva) Playbook. This document is at an advanced stage of completion and includes a list of the critical business functions. DFAM will further enhance this document to address the audit recommendations with respect to recovery time and impact, and to reflect the experience gathered during COVID crisis. The document will constitute the basis for DIST to identify and analyze the necessary supporting IT systems and complete the Business Impact Analysis (BIA). Based on the results

[11] Critical recommendations address those risk issues that require immediate management attention. Failure to take action could have a critical or significant adverse impact on the Organization.

[12] Important recommendations address those risk issues that require timely management attention. Failure to take action could have a high or moderate adverse impact on the Organization.

Rec. no.	Recommendation	Critical[11]/ Important[12]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	based on the results of the business impact analysis.					of the BIA, the Playbook will be updated to reflect the support needed for global IT systems during a crisis. Furthermore, field offices will be advised to include provisions for ensuring continuity of their critical local IT systems in their local BCPs.
3	The UNHCR Division of Information Systems and Telecommunications should ensure that disaster recovery arrangements are in place for all applications and systems that support critical business processes.	Important	Yes	Deputy Director BRMS/ DIST	Q4 2021	Depending on the available of funding, the applications and systems supporting critical processes will be included in disaster recovery arrangements by Q4, 2021.
4	The UNHCR Division of Information Systems and Telecommuncations should explore viable solutions including cloud services for securely storing a copy of the backed-up data for its field offices.	Important	Yes	Deputy Director ICT Operations /DIST	Q2 2021	DIST will explore by Q2, 2021 the most efficient and effectives solutions for securely storing a copy of the back-up data for the field offices.