United Nations Nations Unies

INTEROFFICE MEMORANDUM MEMORANDUM INTERIEUR

OFFICE OF INTERNAL OVERSIGHT SERVICES · BUREAU DES SERVICES DE CONTRÔLE INTERNE

INTERNAL AUDIT DIVISION · DIVISION DE L'AUDIT INTERNE

TO: Mr. António Guterres, High Commissioner
A: United Nations High Commissioner for Refugees

DATE: 15 December 2011

REFERENCE: IAD: 11- 00748

FROM: Fatoumata Ndiaye, Director
DE: Internal Audit Division, OIOS

SUBJECT: **Assignment no. AT2011/166/02 – Audit of the arrangements for business continuity and**
OBJET: **disaster recovery for non-PeopleSoft applications in UNHCR**

Overall results relating to efficiency and effectiveness of disaster recovery and business continuity plans were partially satisfactory

1. Attached please find the final report on the above-mentioned audit.

2. Annex I shows the status of recommendations.

3. Please note that OIOS will report on the progress made to implement its recommendations in its annual report to the General Assembly. OIOS will also report to the Secretary-General quarterly for critical recommendations and annually for important recommendations.

4. We wish to express our appreciation to the Management and staff of UNHCR for the assistance and cooperation extended to the auditors during the assignment.

cc: Mr. Alexander Aleinikoff, Deputy High Commissioner, UNHCR
Ms. Erika Feller, Assistant High Commissioner (Protection), UNHCR
Ms. Janet Lim, Assistant High Commissioner (Operations), UNHCR
Ms. Naginder Dhanoa, Director and CIO, DIST, UNHCR
Ms. Kumiko Matsuura-Mueller, Controller and Director, DFAM, UNHCR
Mr. Stephen Ingles, Deputy Controller, DFAM, UNHCR
Ms. Stephanie Rinville, Audit Coordinator, UNHCR
Mr. Nicholas Birch, Audit Coordinator Assistant, UNHCR
Mr. Swatantra Goolsarran, Executive Secretary, UN Board of Auditors
Mr. Rohan Wijeratne, Board of Auditors
Ms. Susanne Frueh, Executive Secretary, Joint Inspection Unit
Mr. Moses Bamuwamye, Executive Secretary, IAAC
Mr. Zachary Ikiara, Chief, Oversight Support Unit, DM
Mr. Byung-Kun Min, Special Assistant to the USG-OIOS
Mr. Christopher F. Bagot, Chief, Geneva Audit Service, OIOS
Ms. Amy Wong, Programme Officer, Internal Audit Division, OIOS

FINAL AUDIT REPORT

Audit of the arrangements for business continuity and disaster recovery for non-PeopleSoft applications in UNHCR

BACKGROUND

The field offices of the United Nations High Commissioner for Refugees (UNHCR) implement strategies and policies for the protection and assistance of persons of concern (asylum seekers, refugees and internally displaced persons) in the region under their respective jurisdictions. Several information and communications technology (ICT) applications play an essential role in supporting their operations.

UNHCR operates in over 100 countries with 350 field offices, 7,000 staff members and a budget (2011) of $2 billion. The 2011 budget allocation for non-PeopleSoft applications was $5.5 million.

The Division of Information Systems and Telecommunications (DIST), located at UNHCR’s Headquarters in Geneva, is responsible for the maintenance, evolution and support of UNHCR's critical ICT applications. DIST has global responsibility for the proper functioning of the existing ICT systems and for planning new ICT initiatives. A change management project is currently underway to improve ICT services in UNHCR.

The ICT enterprise-wide applications in UNHCR include: (i) enterprise resources planning system (PeopleSoft); (ii) electronic archiving document management system (Livelink); (iii) refugee registration system (proGres); (iv) email system (Novell GroupWise); (v) intranet; and (vi) results-based budgeting system (Focus). Their details are listed in Table 1 below.

Application	Used in	No of users *	Data volume	Hosted by	Purpose
Livelink	HQ and Field	2,500	1.5 TB	UNHCR	Electronic archiving document management system. Roll-out to Europe completed in March 2011. Other locations don’t have access to it.
GroupWise	HQ and Field	11,000	25 TB	UNHCR	Email system: - 1600 mailboxes in HQ; - 2000 mailboxes in centralized post offices; - 7400 mailboxes 160 field locations.
proGres	Field	1,500	1.2 TB	UNHCR	Client/server based application implemented in 81 countries with 300 active instances for the registration of refugees. (Development of a web based system is in progress.)
Intranet	HQ and Field	9,000	100 GB	UNHCR	Managing internal communication and information.
Focus	HQ and Field	10,000	21 GB	UNICC	Supporting the results-based managing system of UNHCR.

*including disabled/inactive users

In addition to the ICT enterprise-wide applications, UNHCR field offices rely on several locally developed applications for supporting specific business requirements.

The PeopleSoft system is supported by a hosting agreement with the United Nations International Computing Centre (UNICC) that includes adequate provisions for business continuity and disaster recovery, recently tested using an off-site location in September 2010. The same level of support and coverage is not in place for non-PeopleSoft applications.

OBJECTIVE AND SCOPE

The audit was conducted to assess the adequacy and effectiveness of UNHCR's risk management, control and governance processes in providing reasonable assurance that disaster recovery and business continuity plans are effective in ensuring that non-PeopleSoft applications can withstand adverse events and can continue to operate within a reasonable time frame in case of interruption. The key controls tested for the audit included: (a) risk management and strategic planning mechanisms; and (b) disaster recovery and business continuity plans. The audit was conducted at the UNHCR Headquarters in Geneva and covered the period from 1 January 2009 to 31 March 2011.

AUDIT RESULTS

In OIOS' opinion, UNHCR's risk management, control and governance processes examined were **partially satisfactory** in providing reasonable assurance regarding the effective implementation and management of business continuity plans and disaster recovery arrangements for non-PeopleSoft applications.

UNHCR established a business continuity plan in 2009 (updated in 2010) as part of the pandemic preparedness programme. The programme included the list of critical staff members, and details for maintaining communications and managing critical business processes remotely. UNHCR successfully performed a test at the end of 2009 at their Headquarters, confirming the effectiveness of the communications and the ability to continue critical business processes remotely (from the staff members' residences). However, several areas require corrective actions, as outlined below.

Risk assessment process for ICT field operations

DIST did not establish risk assessment processes for identifying and mitigating the risks associated with the use of non-PeopleSoft applications supporting the field offices operations. In addition, DIST did not maintain an inventory of locally developed applications. As a result, the continuity of the field offices operations is exposed to threats that have not been adequately identified and assessed.

(1) The UNHCR Division of Information Systems and Telecommunications should lead an initiative for designing and implementing a global ICT risk assessment in all field offices.

(2) The UNHCR Division of Information Systems and Telecommunications, in coordination with the field offices, should develop a central inventory of the locally developed applications supporting field operations.

UNHCR accepted recommendations 1 and 2, stating that it values and respects the audit observations and plans to address the observed gaps. An initial inventory of field-developed applications was made in August/September 2011. Efforts were also underway to upgrade the infrastructure that enabled an automated inventory taking of all applications used in the organization. This system is expected to be in place by the end of 2012. Recommendations 1 and 2 remain open pending development of: (a) a global ICT risk assessment; and (b) an inventory of the locally developed applications supporting field operations.

Disaster recovery planning

UNHCR Headquarters established a service delivery agreement with UNICC for hosting the results-based budgeting system (Focus). However, this agreement did not include provisions for disaster recovery services.

UNHCR field offices did not have a formal plan of action for recovering locally hosted systems that were considered critical to their activities (i.e., electronic messaging and refugee data registration systems). Although some UNHCR field offices (i.e., Jordan and Thailand) have their systems hosted externally with local service providers, the corresponding agreements did not include disaster recovery plans and provisions.

(3) The UNHCR Division of Information Systems and Telecommunications, in coordination with the field offices, should ensure that an adequate disaster recovery plan is in place for the results-based budgeting application (Focus) and those applications considered critical to the activities of the field offices.

UNHCR accepted recommendation 3 and stated that: (i) A set of procedures and processes are prepared for the ProGres system of field office to safeguard data, which will be revised bearing in mind the new structure of the IT Division; (ii) Livelink and intranet backup servers are located in a separate location at the Headquarters, that would be activated automatically in case of an outage. Data backup is conducted every evening; and (iii) No disaster recovery and business continuity plan is required for the field office because the client application and associated data can be downloaded in case of an outage. At the central server level, the Focus database is hosted at the UNICC and a hot backup of the database server is active. Down time would be in the order of one business day (approx 8 hrs) but with the expectancy of little or no data loss. Global Focus is not considered sufficiently mission critical to require a hot standby database and can be rebuilt from the current production (hot backup). OIOS took note of the additional explanations provided by UNHCR with regard to ProGres, Livelink and Focus applications. Recommendation 3 remains open pending receipt of the disaster recovery plans developed for the field systems supporting mail servers (GroupWise), network drives and local applications other than ProGres and Focus.

Satellite connection for field offices

About 100 UNHCR field offices (28 per cent of the total) use satellite communication links as the main connection medium for accessing all enterprise-wide applications (i.e., Focus, Livelink) hosted in the Geneva Headquarters. This connection is routed via a satellite provider located in Germany and linked to the server rooms of the Geneva Headquarters. However, there was no redundancy in case of unavailability of the servers in Geneva Headquarters or the satellite provider's facilities in Germany.

(4) The UNHCR Division of Information Systems and Telecommunications should establish alternative connectivity links and procedures for ensuring the availability of reliable satellite connection between field offices and Geneva Headquarters.

UNHCR accepted recommendation 4 and stated that independent backup links to all offices have been established using local internet service providers and mobile satellite services if terrestrial services are not available. In addition, plans are underway to start implementing the secondary satellite links as of January 2013. Recommendation 4 remains open pending receipt of documented evidence demonstrating the establishment of the independent backup links.

Business continuity plan

UNHCR's business continuity plan is composed of several documents stored in separate repositories (partly in Livelink and partly in the Organization's intranet). Furthermore, the available details pertaining to critical staff members (i.e., contact information) and business processes were not consistent across the various divisions of the Organization.

(5) The UNHCR Division of Information Systems and Telecommunications should store the business continuity plan in centralized and backup repository locations and, in coordination with relevant divisions, ensure that its content is complete, consistent and updated.

UNHCR accepted recommendation 5 stating that steps will be taken for addressing the observed gaps. Recommendation 5 remains open pending receipt of details on the creation of a central and backup repository locations with complete information on business continuity planning.

ACKNOWLEDGEMENT

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.

CONTENTS

I. INTRODUCTION

1. The Office of Internal Oversight Services (OIOS) conducted an audit of the arrangements for the business continuity and disaster recovery of non-PeopleSoft applications in the Office of the United Nations High Commissioner for Refugees (UNHCR) Headquarters in Geneva. Comments made by UNHCR are shown in *italics.*

II. AUDIT OBJECTIVE

2. The audit was conducted to assess the adequacy and effectiveness of UNHCR's risk management, control and governance processes in providing reasonable assurance that disaster recovery and business continuity plans are effective in ensuring that non-PeopleSoft applications can withstand adverse events and can continue to operate within a reasonable time frame in case of interruption. The key controls tested for the audit included: (a) risk management and strategic planning mechanisms; and (b) disaster recovery and business continuity plans. For the purpose of this audit, OIOS defined these key controls as follows:

(a) Risk management and strategic planning - those controls that are designed to provide reasonable assurance that non-PeopleSoft applications are identified and assessed, and that actions are taken to mitigate or anticipate risks.

(b) Disaster recovery and business continuity plans - those controls that are designed to provide reasonable assurance that disaster recovery and business continuity plans exist for ensuring that non PeopleSoft applications can withstand crisis and continue to operate within a reasonable time frame.

III. AUDIT SCOPE AND METHODOLOGY

3. OIOS conducted this audit from April to June 2011. The audit was carried out at the UNHCR Headquarters in Geneva and covered the period from 1 January 2009 to 31 March 2011.

4. To gain a general understanding of the processes of UNHCR's risk management and strategic planning, business continuity and disaster recovery, OIOS conducted interviews with key personnel, and reviewed documentation related to UNHCR network and ICT operations world-wide. OIOS visited the server rooms of UNHCR in two locations in Geneva, and also considered the documentation and information obtained during previous audits of ICT operations in the field offices. The audit team conducted an activity-level risk assessment to identify and evaluate specific risk exposures, and to confirm the relevance of the key controls in mitigating associated risks.

5. Through interviews, analytical reviews and tests of controls, OIOS assessed the existence and adequacy of written policies and procedures, and whether they were implemented consistently.

IV. OVERALL ASSESSMENT

6. In OIOS' opinion, UNHCR's risk management, control and governance processes examined were **partially satisfactory** in providing reasonable assurance regarding the effective implementation and management of business continuity plans and disaster recovery arrangements for non-PeopleSoft applications. Overall, UNHCR had put in place a business continuity and contingency plan in 2009 (updated in April 2010) to deal with the potential pandemic outbreak (Avian flu). UNHCR focused on identifying critical staff members, maintaining communication among them and managing critical business processes remotely. UNHCR successfully performed a test at the end of 2009 confirming the

effectiveness of the communication and the ability to continue critical business processes remotely. However, additional controls should be implemented for establishing a risk assessment process, completing the disaster recovery provisions for the results-budgeting system and the applications used in field offices, and consolidating the documentation and information pertaining to business continuity and disaster recovery plans. In addition, UNHCR should: (a) lead an initiative for designing and implementing a global ICT risk assessment; (b) develop a central inventory of applications developed in the field offices; (c) develop a comprehensive disaster recovery plan; (d) establish alternative satellite connectivity links for field offices; and (e) centralize in a single location the details of the business continuity and disaster recovery plan.

V. AUDIT RESULTS

A. Risk management and strategic planning

Need for a systematic implementation of a risk assessment process

7. Risk assessment is an essential element of the business continuity plan that requires: (i) identification of potential risks; (ii) assessment of the critical functions necessary to continue critical operations; (iii) identification of the controls in place; (iv) assessment of potential impact on operations; and (v) definition of mitigating controls to address the residual risks.

8. UNHCR field offices use non-PeopleSoft applications for supporting their operations in delivering assistance to the persons of concern. These applications include systems locally developed that are considered critical to their field operations. However, an inventory of these applications was not centrally available since the Division of Information Systems and Telecommunications (DIST) does not support locally developed systems. These systems were developed locally with limited supervision from DIST for ensuring consistency and security, and had not been subject to any assessment regarding the tolerable downtime acceptable to each office in case of their unavailability.

9. UNHCR has not planned or conducted any assessment of the risks affecting the continuity and recovery of its operations in case of unavailability of the non-PeopleSoft applications. Although DIST has an overall responsibility for ICT strategic planning and risk assessment, these processes were not supported by adequate governance and control mechanisms.

Recommendations 1 and 2

(1) The UNHCR Division of Information Systems and Telecommunications should lead an initiative for designing and implementing a global ICT risk assessment in all field offices.

(2) The UNHCR Division of Information Systems and Telecommunications, in coordination with the field offices, should develop a central inventory of the locally developed applications supporting field operations.

10. *UNHCR accepted recommendations 1 and 2, stating that it values and respects the audit observations and plans to address the observed gaps. An initial inventory of field-developed applications was made in August/September 2011. Efforts were also underway to upgrade the infrastructure that enabled an automated inventory taking of all applications used in the organization. This system is expected to be in place by the end of 2012.* Recommendations 1 and 2 remain open pending development of: (i) a global ICT risk assessment; and (ii) an inventory of the locally developed applications supporting field operations.

B. Disaster recovery and business continuity plan

11. Disaster recovery planning is a key component of business continuity and pertains to the processes and technologies needed for resuming operations after a disruptive event. The goal of a disaster recovery plan is to restore the operability of systems that support critical business processes. The main components of a disaster recovery plan are: (i) classification of critical processes; (ii) supporting technology infrastructure (applications, data and hardware); (iii) manual procedures; (iv) business impact analysis; (v) recovery time (time to recover) and point (data to recover) objectives; (vi) critical ICT personnel; and (vii) testing.

12. The two main non-PeopleSoft applications in use at the Geneva Headquarters included the document repository system (Livelink) and the results-based budgeting application (Focus). Both of these applications were not supported by documented disaster recovery plans.

13. UNHCR has two data centres in Geneva, where data and systems hosted in these two locations are replicated synchronously. DIST conducts daily, weekly and monthly backups of this data.

14. The following procedures and mechanisms have been established in the event that one of the two data centres would be become unavailable:

(a) Main operations would continue from the alternate location. Since both sites have redundant links and live data, the current setup allows for a failover in the event of link failure; and

(b) Critical processes can be performed by staff members remotely (i.e., from their residence) via Internet connection. Furthermore, UNHCR started a pilot project for introducing a virtual private network (VPN) technology that would allow staff members to access data stored in network drives remotely.

Inadequate disaster recovery planning in field offices

15. The main non-PeopleSoft applications used in UNHCR field offices include the local mail servers (GroupWise), network drives for sharing resources, refugee registration system (proGres), and other locally developed applications. The data contained in these applications is held locally, under the responsibility of the local UNHCR management. UNHCR field offices did not have adequate disaster recovery plans in place for supporting these applications. While regular backups of the data were performed, the backup media were not stored off-site, thereby exposing the office to the risk of data loss should there be a disaster. However, there were no records of data lost in the last two years.

Inadequate disaster recovery planning for externally hosted systems

16. The United Nations International Computing Centre (UNICC) provides hosting services in Geneva, for UNHCR’s results-based budgeting system (Focus). This system is an operations management support software designed to assist UNHCR’s offices in recording operational objectives, defining performance indicators, preparing programme budgets and reporting on the progress made in achieving results. All UNHCR field offices and divisions use Focus. The service delivery agreement established with UNICC for hosting Focus did not include disaster recovery provisions. While UNICC provides disaster recovery support for UNHCR’s Enterprise Resource Planning (ERP) system (PeopleSoft), the same support has not been defined for Focus.

17. Similarly, some field offices (i.e., Jordan, Thailand) that have hosted their systems externally with local service providers, signed agreements that did not include provisions for disaster recovery planning.

Recommendation 3

(3) The UNHCR Division of Information Systems and Telecommunications, in coordination with the field offices, should ensure that an adequate disaster recovery plan is in place for the results-based budgeting application (Focus) and those applications considered critical to the activities of the field offices.

18. *UNHCR accepted recommendation 3 and stated that: (i) A set of procedures and processes are prepared for the ProGres system in field offices to safeguard data, which will be revised bearing in mind the new structure of the IT Division; (ii) Livelink and intranet backup servers are located in a separate location at the Headquarters, that would be activated automatically in case of an outage. Data backup is conducted every evening; and (iii) No disaster recovery and business continuity plan is required for Focus in the field office because the client application and associated data can be downloaded in case of an outage. At the central server level, the Focus database is hosted at the UNICC and a hot backup of the database server is active. Down time would be in the order of one business day (approx 8 hrs) but with the expectancy of little or no data loss. Focus is not considered sufficiently mission critical to require a hot standby database and can be rebuilt from the current production (hot backup).* OIOS took note of the explanations provided by UNHCR with regard to ProGres, Livelink and Focus applications. Recommendation 3 remains open pending receipt of the disaster recovery plans developed for the field systems supporting mail servers (GroupWise), network drives and local applications other than ProGres and Focus.

No connectivity redundancy for field offices connecting through satellite

19. About 100 UNHCR field offices (28 per cent of the total) use satellite communication links as the main connection medium for accessing all enterprise-wide applications (i.e., Focus, Livelink) hosted in the Geneva Headquarters. This connection is routed via a satellite provider located in Germany and linked to the server rooms of the UNHCR Geneva Headquarters. However, there was no redundancy in case of unavailability of the servers in the main building or the satellite provider's facilities in Germany.

20. DIST acknowledged the risks deriving from the lack of alternative solutions for satellite connectivity with field offices. Several field offices experienced problems and unavailability of satellite connectivity on a regular basis. In this regard, email messages are broadcast on the UNHCR email system informing the user community of the temporary unavailability of connectivity with field offices. On average, the service unavailability ranges from 24 to 72 hours. Although, in some cases (i.e., UNHCR Chad in June/July 2010 and Congo Brazaville in May 2011) the connection was unavailable for longer periods (five days for Chad and eleven days for Congo Brazaville). The lack of reliable connectivity had a negative impact on the operations of the offices and posed increased security risks to staff members working in remote locations.

Recommendation 4

(4) The UNHCR Division of Information Systems and Telecommunications should establish alternative connectivity links and procedures for ensuring the availability of reliable satellite connection between field offices and Geneva Headquarters.

21. *UNHCR accepted recommendation 4 and stated that independent backup links to all offices have been established using local internet service providers and mobile satellite services if terrestrial services*

are not available. In addition, plans are underway to start implementing the secondary satellite links as of January 2013. Recommendation 4 remains open pending receipt of documented evidence demonstrating the establishment of independent backup links.

Need to update the business continuity plan

22. Business continuity planning refers to the process of establishing advance arrangements and procedures that would enable an organization to continue its operations irrespective of adverse circumstances or events. The main components of a business continuity plan are: (i) people; (ii) premises; (iii) technology; (iv) data; (v) supplies; and (vi) stakeholders.

23. UNHCR established a business continuity plan in 2009 (updated in 2010) as part of the pandemic preparedness programme. The programme included the list of critical staff members and details for maintaining communications and managing critical business processes remotely. A test was successfully performed at the end of 2009 at their Headquarters for confirming the effectiveness of the communications and the ability to continue critical business processes remotely (from the staff members' residences). However, while the results of the test were successful, several areas for improvement were identified.

24. The details of UNHCR's business continuity plan were included in several documents stored in separate repositories (partly in Livelink and partly in the Organization's intranet). Furthermore, the details pertaining to critical staff members, contact information and key business processes were not consistently available for all the divisions of the Organization. Some of the key personnel who were involved in the plan have since then moved to other functions or locations, but their information were not updated.

Recommendation 5

(5) The UNHCR Division of Information Systems and Telecommunications should store the business continuity plan in centralized and backup repository locations and, in coordination with relevant divisions, ensure that its content is complete, consistent and updated.

25. *UNHCR accepted recommendation 5 stating steps will be taken for addressing the observed gaps.* Recommendation 5 remains open pending receipt of details on the creation of a central and backup repository locations with complete information on business continuity planning.

ANNEX I
STATUS OF RECOMMENDATIONS
Audit of the arrangements for business continuity and disaster recovery for non-PeopleSoft applications in UNHCR

Recom. no.	Recommendation	Risk category	Critical/ important	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
1	The UNHCR Division of Information Systems and Telecommunications should lead an initiative for designing and implementing a global ICT risk assessment in all field offices..	Operational	Important (Medium)	O	Provide evidence of the global ICT risk assessment.	31/December/ 2012
2	The UNHCR Division of Information Systems and Telecommunications, in coordination with the field offices, should develop a central inventory of the locally developed applications supporting field operations.	Information resources	Important (Medium)	O	Provide evidence of the inventory of locally developed applications supporting field operations.	31/December/ 2012
3	The UNHCR Division of Information Systems and Telecommunications, in coordination with the field offices, should ensure that an adequate disaster recovery plan is in place for the results-based budgeting application (Focus) and those applications considered critical to the activities of the field offices.	Operational	Important (Medium)	O	Provide evidence of the disaster recovery plan developed for the locally hosted applications considered critical to the activities of the field offices (mail servers, shared drives, etc.)	30/June/2013
4	The UNHCR Division of Information Systems and Telecommunications should establish alternative connectivity links and procedures for ensuring the availability of reliable satellite connection between field offices and Geneva Headquarters.	Operational	Important (Medium)	O	Provide evidence of the establishment of independent backup links.	31/January/2013
5	The UNHCR Division of Information Systems and Telecommunications should store the business continuity plan in a centralized and backup repository locations and, in coordination with relevant divisions, ensure that its content is complete, consistent and updated.	Operational	Important (Medium)	O	Provide evidence of the central repository and backup locations created for storing the business continuity plan.	31/December/ 2012

[1] C = Closed, O = Open

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