Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2015/112

Audit of information and communication technology hosting services provided by third parties to the Office of the United Nations High Commissioner for Refugees

Overall results relating to the effective management of information and communication technology hosting services provided by third parties were initially assessed as partially satisfactory. Implementation of three important recommendations remains in progress

FINAL OVERALL RATING: PARTIALLY SATISFACTORY

30 September 2015
Assignment No. AR2015/166/01

CONTENTS

AUDIT REPORT

Audit of information and communication technology hosting services provided by third parties to 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 and communication technology (ICT) hosting services provided by third parties to the Office of the United Nations High Commissioner for Refugees (UNHCR).

2. In accordance with its mandate, OIOS provides assurance and advice on the adequacy and effectiveness of the United Nations internal control system, the primary objectives of which are to ensure (a) efficient and effective operations; (b) accurate financial and operational reporting; (c) safeguarding of assets; and (d) compliance with mandates, regulations and rules.

3. The concept of hosting services is based on an outsourcing arrangement whereby a service provider will host information systems or resources on behalf of a client. These systems and resources are then accessed by the client over a dedicated network or the Internet. It is a business model used for delivering ICT services.

4. Within the UNHCR Division of Information Systems and Telecommunications (DIST), ICT Operations, a service operating out of Amman, Jordan, has the overall responsibility for designing, delivering and maintaining the common ICT infrastructure which is the foundation of all services provided by DIST. The ICT Platform Section, under ICT Operations, manages hosting services, and its terms of reference include: (a) managing the hosting arrangements with outsourced service providers and ensuring that these services are provided to the agreed service levels; and (b) providing increased efficiencies and cost reductions, while remaining fit for purpose.

5. The corporate ICT systems of UNHCR are currently hosted in a United Nations entity and a private sector service provider. The United Nations entity owns the hardware and hosts the mission-critical systems such as: Managing for Systems, Resources and People (MSRP), the UNHCR enterprise resource planning system; FOCUS, the UNHCR results-based management system; and the UNHCR public website (unhcr.org). The private sector service provider hosts Microsoft Exchange, another mission-critical system for UNHCR messaging services. This service provider also hosts: the development and production environments of the proGres system, the UNHCR refugee registration system; eSAFE, the UNHCR document management system; and part of the UNHCR wide area network/Internet connectivity and Hyper-V, a virtual server farm. UNHCR owns and provides the hardware for these services while the private sector entity provides the facilities such as the premises, air conditioning, power and connectivity.

6. The total payment that UNHCR made to the private sector hosting service provider in both 2013 and 2014 was $450,000. The payment to the United Nations entity for 2013 and 2014 was $3.4 million. The written down value of ICT assets located at the premises of the private sector entity amounted to $400,000 as at 31 December 2014, while their acquisition cost was $1.3 million.

7. Comments provided by UNHCR are incorporated in *italics*.

II. OBJECTIVE AND SCOPE

8. The audit was conducted to assess the adequacy and effectiveness of UNHCR governance, risk management and control processes in providing reasonable assurance regarding the **effective management of information and communication technology hosting services provided by third parties**.

9. This audit was included in the OIOS 2015 risk-based internal audit work plan for UNHCR because of the risks associated with relying on third parties hosting mission-critical ICT systems for UNHCR.

10. The key controls tested for the audit were: (a) strategic planning; (b) performance monitoring; and (c) ICT support systems. For the purpose of this audit, OIOS defined these key controls as follows:

(a) **Strategic planning** - controls that provide reasonable assurance that DIST has developed a strategic plan to implement its organizational objectives for ICT services, including those outsourced to third party hosting service providers.

(b) **Performance monitoring** - controls that provide reasonable assurance that metrics are established to monitor third party hosting service providers and to ensure that provisions in the relevant service level agreements are complied with.

(c) **ICT support systems** - controls that provide reasonable assurance that the ICT systems supporting UNHCR operations exist and are physically secure.

11. The key controls were assessed for the control objectives shown in Table 1.

12. OIOS conducted the audit from February to June 2015. The audit covered the period from 1 January 2013 to 31 December 2014.

13. OIOS conducted an activity-level risk assessment to identify and assess specific risk exposures, and to confirm the relevance of the selected key controls in mitigating associated risks. Through interviews and analytical reviews, OIOS assessed the existence and adequacy of internal controls and conducted necessary tests to determine their effectiveness.

III. AUDIT RESULTS

14. The UNHCR governance, risk management and control processes examined were initially assessed as **partially satisfactory**[1] in providing reasonable assurance regarding the **effective management of information and communication technology hosting services provided by third parties**. OIOS made three recommendations to address the issues identified.

15. There was a need for UNHCR to: (a) update the ICT strategy to reflect the use of hosting and cloud services; (b) implement measures to facilitate physical verification of assets located at the site of the private sector hosting service provider; and (c) store off-site the information held in the premises of the private sector hosting service provider.

[1] A rating of **"partially satisfactory"** means that important (but not critical or pervasive) deficiencies exist in governance, risk management or control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

16. The initial overall rating was based on the assessment of key controls presented in Table 1. The final overall rating is **partially satisfactory** as implementation of three important recommendations remains in progress.

Table 1: Assessment of key controls

Business objective	Key controls	Control objectives			
		Efficient and effective operations	**Accurate financial and operational reporting**	**Safeguarding of assets**	**Compliance with mandates, regulations and rules**
Effective management of information and communication technology hosting services provided by third parties	(a) Strategic planning	Partially satisfactory	Partially satisfactory	Partially satisfactory	Partially satisfactory
	(b) Performance monitoring	Satisfactory	Satisfactory	Satisfactory	Satisfactory
	(c) ICT support systems	Partially satisfactory	Partially satisfactory	Partially satisfactory	Partially satisfactory
FINAL OVERALL RATING: PARTIALLY SATISFACTORY					

A. Strategic planning

The information and communication technology strategy should be updated to reflect the use of hosting and cloud services

17. The UNHCR Global Management and Accountability Framework requires DIST to design, update and implement an ICT strategy that responds to the evolving demands of UNHCR and to ensure that ICT investments are aligned and prioritized with operational needs. In line with this responsibility, the UNHCR ICT strategy, which was last updated in October 2012, specifies that DIST consider alternative options for a coherent approach to infrastructure hosting to reduce costs and risk exposures.

18. A review of the 2012 ICT strategy showed that although it referred to hosting services, the document lacked relevant detail, such as the planned goals and the resources required, and did not refer to modalities for implementing the strategy. In contrast, the previous ICT strategy for 2008-2011 had specifically referred to determining options and costs for using external partners to host file servers, reviewing the performance of the United Nations entity for hosting the MSRP, and reviewing possible hosting solutions for headquarters servers and future provisioning strategy for servers. Further, although the ICT Platform Section was expected to provide a long-term strategy for the use of "cloud services" across UNHCR, this had not been done.

19. The lack of clarity concerning the UNHCR approach to use of hosting and cloud services occurred because the ICT strategy had not been updated for more than three years to reflect important and relevant developments.

(1) The UNHCR Division of Information Systems and Telecommunications should update the UNHCR information and communication technology strategy to adequately reflect the use of hosting and cloud services.

UNHCR accepted recommendation 1 and stated that the 2012 ICT strategy would be updated to

address the intended direction of hosting/cloud services at a strategic level. The specific implementation activities, along with the details concerning budget and resources would continue to be addressed in the DIST Annual Programme Review document. Recommendation 1 remains open pending receipt of the updated ICT strategy that adequately reflects the use of hosting and cloud services.

B. Performance monitoring

Adequate arrangements were in place for monitoring service delivery levels for hosting services in accordance with the agreements with the service providers

20. The Operational Guidelines on ICT Security specify that DIST, in close coordination with responsible UNHCR managers, should define and monitor service and delivery levels as well as security controls provided by third party providers supporting UNHCR information processing and telecommunication services to ensure that the services are implemented, operated and maintained in accordance with contractual obligations.

21. A review of the arrangements for performance monitoring of service delivery by the United Nations and the private sector ICT hosting service providers showed that the ICT Platform Section adequately monitored the service delivery by both providers, based on periodic reports received and regular meetings held with both entities. For example, the United Nations entity collected and published, on a monthly basis, service availability metrics which allowed UNHCR to measure the actual performance against service level targets and to compare the services with those offered by other service providers in the industry. UNHCR had also established adequate arrangements to monitor the agreement with the private sector entity under which facilities such as premises, air-conditioning, power and connectivity were provided. Temperature fluctuations and power outages were monitored by the technical staff of the private sector entity, and any events in this regard were published on their website and were thus accessible for review by DIST staff. No significant incidents of power outages or air-conditioning problems had been reported. OIOS therefore concluded that adequate arrangements were in place for monitoring service delivery levels for ICT hosting services.

Audit reports provided the required assurance on internal controls at the United Nations entity

22. The International Standard on Assurance Engagements 3402 on Assurance Reports on Controls at a Service Organization requires service providers to provide an assurance report over a specified period to its user entities and their auditors on the controls established that are likely to impact or be part of the system of internal control at the user entities.

23. In line with industry best practice, the United Nations entity pursued a number of relevant control certifications and independent audits based on international standards to ensure that a complete and effective set of operational controls were in place. OIOS review of the audit reports received by UNHCR for 2013 and 2014 concluded that the United Nations entity had established satisfactory controls and the reports provided positive opinions on the adequacy of the ICT hosting arrangements. The agreement between UNHCR and the private sector entity did not contain such an audit clause, and no separate assurance reports were considered necessary since this was a contract for the provision of premises, air-conditioning, power and connectivity for hosting UNHCR-owned and controlled hardware. In addition, the private sector entity provided the required services in accordance with the agreement and authorized UNHCR representatives had access to the ICT equipment located in its premises.

C. Information and communication technology support systems

Measures needed to be implemented to facilitate physical verification of assets located at the site of the private sector hosting service provider

24. The UNHCR Manual specifies that once an item of property, plant and equipment (PPE) has been procured and delivered to a UNHCR office, it needs to be registered, tracked and managed until disposed of. Furthermore, each asset should be physically verified at least once a year to reconcile all assets recorded in the MSRP Asset Management Module with the physical holding and to provide the latest information on the location of the PPE and their working condition.

25. DIST stated that its assets in the premises of the private sector hosting service provider were physically verified in November 2014 and submitted a spreadsheet to corroborate the exercise performed. OIOS visited the private sector entity to physically verify the ICT assets hosted in its premises and observed that although the assets had barcode labels, only a few of those barcodes were visible externally. OIOS was able to physically verify only 12 of the more than 100 servers and devices. This was because the barcode labels for most of the live assets (such as servers) were affixed inside the enclosures of the equipment, and therefore could only be reviewed when the server or another device was shut down and removed from its docking position. Such an action was not possible at the time of the verification exercise as it would have disrupted the ICT services.

26. DIST had not adequately considered the constraints in its physical verification of assets and should have established a workaround to address the issue, such as using technology (e.g., pinging the servers to confirm their existence or running scripts) or displaying asset identifications using hanging tags.

(2) The UNHCR Division of Information Systems and Telecommunications should use hanging tags as a solution to display the asset identification number from Managing for Systems, Resources and People for its assets in the custody of the private sector hosting service provider or use technology such as pinging the servers or running scripts to confirm their existence.

UNHCR accepted recommendation 2 and stated that DIST would work with the managed service providers to ensure that for the new equipment installed, physical tags are identifiable at data centre locations. For the existing equipment, this would only be possible at the next major scheduled maintenance. Recommendation 2 remains open pending receipt of evidence that hanging tags have been used to display the asset identification number for assets in the custody of the private sector hosting services provider or, alternatively, that technology is used to confirm their existence.

Off-site storage measures were required for information stored in the premises of the private sector hosting service provider

27. UNHCR ICT Security Operational Guidelines state that DIST, in close coordination with responsible UNHCR managers, should ensure that adequate and reliable backup and recovery procedures are in place, tested, stored and monitored for all ICT systems. Best practices for ICT, such as CoBiT and ISO/IEC 27001, recommend that, to protect against loss of data, UNHCR should have a sound backup policy and establish procedures to take regular backup copies of information and software. Such backup copies should be stored off-site and tested from time to time.

28. OIOS assessed through interviews with DIST officials that controls relating to off-site storage of information contained in the devices hosted with the private sector hosting service provider were not adequate. For example, backup copies of data were not stored off-site.

29. This situation occurred because appropriate procedures for off-site storage had not been established since DIST perceived the risk as low. DIST explained that the risk of losing data due to a hardware failure practically did not exist, as there was sufficient redundancy in that respect. DIST also explained that other solutions such as file system snapshotting and data protection managers put in place guaranteed against loss of data. However, in the opinion of OIOS, the established backup measures were applicable for on-site storage only and therefore did not entirely eliminate the risk of data loss.

(3) The UNHCR Division of Information Systems and Telecommunications should establish and implement off-site storage procedures for information stored in the premises of the private sector hosting service provider that are consistent with operational requirements.

UNHCR accepted recommendation 3 and stated that DIST had implemented off-site tape storage for eSAFE and was in the process of doing the same for proGres v4 and the Biometric Identify Management System. Recommendation 3 remains open pending confirmation of the implementation of off-site storage procedures for all information stored in the premises of the private sector hosting service provider.

IV. ACKNOWLEDGEMENT

30. 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*) David Kanja
Assistant Secretary-General, Acting Head
Office of Internal Oversight Services

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of information and communication technology hosting services provided by third parties to the Office of the United Nations High Commissioner for Refugees

Recom. no.	Recommendation	Critical[1]/ Important[2]	C/ O[3]	Actions needed to close recommendation	Implementation date[4]
1	The UNHCR Division of Information Systems and Telecommunications should update the UNHCR information and communication technology strategy to adequately reflect the use of hosting and cloud services.	Important	O	Submission to OIOS of the updated ICT strategy that adequately reflects the use of hosting and cloud services.	31 December 2015
2	The UNHCR Division of Information Systems and Telecommunications should use hanging tags as a solution to display the asset identification number from Managing for Systems, Resources and People for its assets in the custody of the private sector hosting service provider or use technology such as pinging the servers or running scripts to confirm their existence.	Important	O	Submission to OIOS of documentary evidence that hanging tags have been used to display the asset identification number for assets in the custody of the private sector hosting service provider or, alternatively, that technology is used to confirm their existence.	31 December 2015
3	The UNHCR Division of Information Systems and Telecommunications should establish and implement off-site storage procedures for information stored in the premises of the private sector hosting service provider that are consistent with operational requirements.	Important	O	Submission to OIOS of documentation confirming implementation of off-site storage procedures for all information stored in the premises of the private sector hosting service provider.	31 December 2015

[1] Critical recommendations address critical and/or pervasive deficiencies in governance, risk management or control processes, such that reasonable assurance cannot be provided with regard to the achievement of control and/or business objectives under review.
[2] Important recommendations address important (but not critical or pervasive) deficiencies in governance, risk management or control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.
[3] C = closed, O = open
[4] Date provided by UNHCR in response to recommendations.

APPENDIX I

Management Response

APPENDIX I

Management Response

Audit of information and communication technology hosting services provided by third parties to the Office of the United Nations High Commissioner for Refugees

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	The UNHCR Division of Information Systems and Telecommunications should update the UNHCR information and communication technology strategy to adequately reflect the use of hosting and cloud services.	Important	Yes	Chief Information Officer (CIO)	31 December 2015	The 2012 ICT Strategy which is currently being updated, will address the intended direction of hosting/cloud services at a strategic level. The specific implementation activities, along with the details concerning budget, resources etc. will continue to be addressed in the DIST Annual Program Review document.
2	The UNHCR Division of Information Systems and Telecommunications should use hanging tags as a solution to display the asset ids from Managing for Systems, Resources and People for its assets in the custody of the private sector hosting services provider or use technology such as pinging the servers or running scripts to confirm their existence.	Important	Yes	Senior ICT Officer (Cross Functional)	31 December 2015	DIST will work with the Managed Service Providers to ensure that for the new equipment installed, physical tags are identifiable at data centre locations in the future. For the existing equipment this may only be possible at the next major scheduled maintenance.
3	The UNHCR Division of Information Systems and Telecommunications should establish and implement off-site storage procedures for information stored in the premises of the private sector hosting services provider that are consistent with operational requirements.	Important	Yes	Deputy Director, ICT Operations	31 December 2015	DIST has implemented off-site tape storage for eSAFE and is in the process of doing the same for proGres v4 and Biometric Identify Management System.

[1] Critical recommendations address critical and/or pervasive deficiencies in governance, risk management or control processes, such that reasonable assurance cannot be provided with regard to the achievement of control and/or business objectives under review.

[2] Important recommendations address important (but not critical or pervasive) deficiencies in governance, risk management or control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.