OIOS

Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2014/129

Audit of the management of externally provided information systems services in the Office of the United Nations High Commissioner for Refugees

Overall results relating to management of externally provided information systems services in the Office of the United Nations High Commissioner for Refugees were initially assessed as partially satisfactory. Implementation of two important recommendations remains in progress.

FINAL OVERALL RATING: PARTIALLY SATISFACTORY

9 December 2014
Assignment No. AR2014/166/01

CONTENTS

AUDIT REPORT

Audit of the management of externally provided information systems services in the Office of the United Nations High Commissioner for Refugees

I.   BACKGROUND

1.   The Office of Internal Oversight Services (OIOS) conducted an audit of the management of externally provided information systems services in 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 Division of Information Systems and Telecommunications (DIST) is responsible for the maintenance, evolution and support of the critical information and communication technology (ICT) systems at UNHCR and also undertakes advance planning to meet the requirements related to UNHCR reliance on information technology through new ICT project initiatives. The Division's October 2012 strategy document stated that the mission of DIST is to provide a world class service that delivers value to UNHCR. DIST is in the process of shifting its focus from directly providing services and is increasingly engaging external partners to provide managed services. Under this initiative, DIST is developing and maintaining the internal skills necessary to identify ICT opportunities, to find the best solutions for the organization, as well as to manage external service providers.

4.   UNHCR entered into managed services agreements with two major vendors, one for application support and maintenance and the other for infrastructure support and maintenance. The application support and maintenance agreement was concluded at the end of 2011 and had been operational for two years, while the agreement for infrastructure support and maintenance was concluded only at the end of 2013 and was in the transition stage at the time of audit.   The total expenditure for managed services amounted to $7 million for the years 2012 and 2013.

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

II.   OBJECTIVE AND SCOPE

6.   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 externally provided information systems services in UNHCR**.

7.   This audit was included in the 2014 risk-based internal audit work plan for UNHCR because of the risks associated with the conclusion of agreements with and the increasing reliance on third parties for services hitherto provided by DIST.

8.   The key control tested for the audit was regulatory framework. For the purpose of this audit, OIOS defined regulatory framework as controls that provide reasonable assurance that policies and procedures related to externally provided information systems services exist and are adequate and effective.

9.   The key control was assessed for the control objectives shown in Table 1.

10.   OIOS conducted this audit from February to June 2014. The audit covered the period from 1 January 2012 to 31 December 2013.

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

III.   AUDIT RESULTS

12.   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 externally provided information systems services in UNHCR**. OIOS made four recommendations to address issues identified in the audit.

13.   Regulatory framework was assessed as partially satisfactory because staff members responsible for receiving ICT services from a vendor performed their certifying functions off-line, resulting in the risk of incorrect certification for the receipt of goods and services. Secondly, there was no designated staff member in DIST to monitor the actions of the vendor's database administrators who had significant privileges and access to mission critical systems. Thirdly, the LANDESK system, an integrated service management tool for UNHCR, was not adequately utilized to monitor services expected against services delivered by the managed services providers. Lastly, there were staff members in DIST who had administrative privileges to some servers while such privileges should have been restricted to the vendor.

14.   The initial overall rating was based on the assessment of key control presented in Table 1 below. The final overall rating is **partially satisfactory** as implementation of two important recommendations remains in progress.

Table 1
Assessment of key control

Business objective	Key control	Control objectives			
		Efficient and effective operations	**Accurate financial and operational reporting**	**Safeguarding of assets**	**Compliance with mandates, regulations and rules**
Effective management of externally provided information systems services	Regulatory framework	Partially satisfactory	Partially satisfactory	Partially satisfactory	Partially satisfactory
FINAL OVERALL RATING: PARTIALLY SATISFACTORY					

---

[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

Regulatory framework

Action was taken to assign roles in Managing for Systems, Resources and People system to strengthen the receiving function

15.   According to the UNHCR Financial Internal Control Framework, the confirm delivery function demonstrates accountability for the outputs and ensures that value for money has been received before payment is made. Staff members who perform this function are given the functional role of receiver. Payments should be made only after certification that contracted goods or services have been received.

16.   During 2012 and 2013, UNHCR paid $3 million for a managed services agreement for application support and for handling enhancements or change requests involving new reports, creation of new fields and added functionalities for the Managing for Systems, Resources and People (MSRP) system, the UNHCR enterprise resource planning system, and Focus, the UNHCR results based management system. The Service Development Section (SDS) in DIST had put in place procedures for processing such enhancement or change requests and the related migration of changes, after testing, to the production system.

17.   However, the SDS team, which was technically qualified to review and accept the work performed by the vendor, was not responsible for certifying the receipt of services directly in the MSRP system. This function was performed in MSRP by the Resources Management Team in DIST based on email correspondence with the SDS team and approval of the time sheets submitted by the vendor. In such off-line certifications, the probability of losing or incorrectly archiving the email exchanges on the subject remained high as no clear policies and procedures existed to deal with such cases. Consequently, there was a risk of incorrect certification for the receipt of goods and services since the receiving function in MSRP was being performed by individuals who had not received the services. This occurred because the SDS team had not been assigned the receiving role in MSRP.

> **(1) The UNHCR Division of Information Systems and Telecommunications should assign the necessary roles to the Service Development Section staff members to perform the receiving function directly in the Managing for Systems, Resources and People system.**
>
> *DIST accepted recommendation 1 and stated that five staff members from the SDS team had been given the necessary roles to perform the receiving function directly in MSRP.* Based on the action taken by DIST, recommendation 1 has been closed.

Action was taken to reassess resource requirements to manage the outsourced database administration function

18.   A database administrator (DBA) is the person responsible for the administration, development, maintenance and implementation of the policies and procedures necessary to ensure the security and integrity of mission critical systems like MSRP and Focus (the UNHCR system for results-based management). A DBA should have the necessary experience, technical expertise and be proactive in identifying problems for resolution and preventing their recurrence. The tasks of the DBA include providing technical support for all database applications in development and production, performing trouble-shooting tasks (such as root cause analysis and code review) and providing a basis for the management of user privileges and roles for security. In view of the importance of this role, UNHCR had previously assigned two staff experienced in Oracle (at P-4 and P-3 levels) for this function. However, with the restructuring of DIST, these positions were discontinued at the end of 2011. Since the beginning

of 2012, the DBA functions had been performed by a vendor for application support and maintenance under the managed services agreement.

19.   A review of the DBA function disclosed that the assigned DBAs:

- lacked Oracle DBA administration skills since they were either system administrators or technical developers but not Oracle DBAs (this skill was required to replace the discontinued function in UNHCR);

- were not proactive in identifying and correcting performance degradation issues such as long running and abnormal processes;

- did not perform root cause analysis for problems; and

- did not perform code reviews or fine tuning of codes.

20.   The situation described above exposed UNHCR to a risk of system errors and non-availability for the following reasons: (a) the DBAs had considerable privileges to the systems and the data and, therefore, their actions needed to be monitored; (b) the DBA function had been outsourced but not 'managed' as there was no designated staff member in DIST to monitor the actions of the vendor's DBA team; and (c) an earlier OIOS audit in 2013 on the planning, delivery and monitoring of the information system services provided by DIST concluded that UNHCR had not established procedures to monitor the actions of users with extended privileges (such as super users and administrators) in MSRP. This occurred because UNHCR lacked the requisite human resources to manage the DBA function being performed by a vendor under the managed services agreement.

> **(2) The UNHCR Division of Information Systems and Telecommunications should ensure that staff members with the appropriate skills, including on database administration, are available in-house to manage service providers rendering database administration services.**
>
> *DIST accepted recommendation 2 and stated that a staff member from the SDS team had been requested to temporarily assume the duty of managing and supervising the vendor provided managed services in the field of PeopleSoft Administration and Database Administration until permanent arrangements would be finalized.* Based on the action taken by DIST, recommendation 2 has been closed.

Limitations in the utilization of the integrated service management tool needed to be addressed

21.   ICT standards require the establishment of a service desk function, for user interface with ICT, to register, communicate, dispatch and analyse all calls, reported incidents, service requests and information demands. Further, there should be monitoring and escalation procedures based on agreed-upon service levels and measurement of end users' satisfaction with the quality of the service desk and ICT services.

22.   UNHCR utilized a system called LANDESK for service management at a cost of about $400,000 during 2012 and 2013 for the licences and maintenance of the product. This system was used to record, track and resolve incidents and problems raised by users and the resulting changes or modifications or enhancements. The data in LANDESK was used to monitor the performance of managed services providers and to track the changes made to the production systems. The vendor delivering infrastructure support services utilized the 'Remedy' system as an integrated service management tool.

23.   A review of existing arrangements showed that:

- The LANDESK system was used only for incident management and desktop support. Most of its other functionalities remained unused including the linking of incidents to recurring problems for root cause analysis or implementing system changes, modifications or enhancements.

- DIST could not adequately utilize LANDESK to monitor the performance of the managed services vendor who provided application support and maintenance. The agreement with the vendor covered enhancements that required less than 40 hours of work in a month. Any enhancement that required over 40 hours or work was outside the scope of the agreement and required a different process to be followed, including a separate statement of work and purchase order. LANDESK was unable to provide details of the change requests processed for critical systems such as MSRP that required less than 40 hours of work. For example, there were 70 changes recorded in the Finance and Supply Chain modules of MSRP between 1 January 2012 and 31 December 2013. However, LANDESK had no information on how many of these changes were performed within 40 hours or if these could be systematically tracked to incidents or change requests. This was mainly due to inconsistent data recording.

- DIST did not ensure that infrastructure support services provided by the managed services agreement were effectively captured in a single system. The vendor manually logged into Remedy all the change requests relating to infrastructure services received from UNHCR users. As a result, the process was subject to errors and data inconsistencies between the two systems. In addition, there was a risk that the vendor would only report on the changes and incidents that were recorded in Remedy and not on all the change requests relating to infrastructure for which it was responsible.

24.   Since relevant service level data was not captured in the LANDESK system, DIST was not able to undertake a proper verification of services expected against services delivered by the managed services providers. The main reasons for the shortcomings discussed above were the absence of technical integration (such as for the free flow of data between LANDESK and Remedy) and the inadequate utilization of all LANDESK system functionalities.

---

(3) The UNHCR Division of Information Systems and Telecommunications should implement an integrated service management tool that provides the means to record and monitor all aspects of the agreements entered into with different service providers.

DIST accepted recommendation 3 and stated that it had reviewed the original strategy and decided not to proceed with the full LAN Desk/Remedy integration as originally planned. A series of work-around processes had been implemented with the vendor and deemed adequate for the moment. The decision would be reviewed by the second quarter of 2015, once the new DIST structure would be staffed and operational, and once the UNHCR Connect & Collaborate initiative with the vendor support had been further rolled-out to field offices. Recommendation 3 remains open pending the implementation of an integrated service management tool after completion of the roll-out of the Connect & Collaborate project to the field offices.

<u>Need to review the administrative rights of user groups</u>

25.   The Information Systems Audit and Control Association indicates that system administration in outsourced functions, such as network security and data centres, should be assigned only to the team members of the managed services provider.

26.   The managed services provider was responsible for managing and running the data centres, corporate email and network security. However, DIST did not ensure that the administrative rights had been uniquely assigned to the vendor's team. There were groups in DIST that still held the administrative rights to the servers and various network devices along with the vendor's team members. DIST had not comprehensively reviewed the assignment of the related administrative rights. In line with its ICT strategy, DIST should focus on the management of the managed services providers rather than performing some of the tasks itself. Since system administration rights should be exclusively vested with the managed services provider, the retention of such rights in DIST could lead to lack of accountability.

<div style="border:1px solid black; padding:10px;">

(4) The UNHCR Division of Information Systems and Telecommunications should review and revoke the administrative rights of all user groups except for the vendor providing the infrastructure services.

DIST accepted recommendation 4 and stated that certain components of the DIST infrastructure in scope for the vendor services were still undergoing the stabilization phase foreseen in the contract. Of the approximately 350 devices/servers already handed over to the vendor, DIST was currently maintaining administrative rights only to approximately 35 items. Write administrative access to these devices would be revoked once the stabilization phase was completed. Hand over/knowledge transfer to the managed services provider for infrastructure would be concluded by the end of the first quarter of 2015, by which time DIST staff members' administrative access would be revoked. Recommendation 4 remains open pending receipt of documentary evidence confirming that no DIST staff members have administrative access to the devices and servers handed over to the managed services provider.

</div>

IV.   ACKNOWLEDGEMENT

27.   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 for Internal Oversight Services

STATUS OF AUDIT RECOMMENDATIONS

**Audit of the management of externally provided information systems services in the Office of the
United Nations High Commissioner for Refugees**

Recom. no.	Recommendation	Critical[2]/ Important[3]	C/ O[4]	Actions needed to close recommendation	Implementation date[5]
1	The UNHCR Division of Information Systems and Telecommunications should assign the necessary roles to the Service Development Section staff members to perform the receiving function directly in the Managing for Systems, Resources and People system.	Important	C	Action taken	Implemented
2	The UNHCR Division of Information Systems and Telecommunications should ensure that staff members with the appropriate skills, including on database administration, are available in-house to manage service providers rendering database administration services.	Important	C	Action taken	Implemented
3	The UNHCR Division of Information Systems and Telecommunications should implement an integrated service management tool that provides the means to record and monitor all aspects of the agreements entered into with different service providers.	Important	O	Submission to OIOS of documentary evidence of the implementation of an integrated service management tool after completion of the roll-out of the Connect & Collaborate project to the field offices.	30 June 2015
4	The UNHCR Division of Information Systems and Telecommunications should review and revoke the administrative rights of all user groups except for the vendor providing the infrastructure services.	Important	O	Submission to OIOS of documentary evidence confirming that no DIST staff members have administrative access to the devices and servers handed over to the managed services provider.	31 March 2015

---

[2] Critical recommendations address significant and/or pervasive deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance cannot be provided regarding the achievement of control and/or business objectives under review.

[3] Important recommendations address important deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

[4] C = closed, O = open

[5] Date provided by DIST in response to recommendations.

APPENDIX I

Management Response

Management Response

**Audit of the management of externally provided information systems services in the Office of the United Nations
High Commissioner for Refugees**

Rec. no.	Recommendation	Critical[6]/ Important[7]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	The UNHCR Division of Information Systems and Telecommunications should assign the necessary roles to the Service Development Section staff members to perform the receiving function directly in the Managing for Systems, Resources and People system.	Important	Yes	Resource Manager, DIST	November 2014	Five staff members from the Service Development and Support team have been given the necessary roles to perform the receiving function directly in MSRP.
2	The UNHCR Division of Information Systems and Telecommunications should ensure that staff members with the appropriate skills, including on database administration, are available in-house to manage service providers rendering database administration services.	Important	Yes	Chief, ICT Service Development and Support Section, DIST	September 2014	Staff member from the Service Development and Support team in Budapest has been requested by the CIO & Director to temporary assume the duty of managing and supervising the vendor provided DBA Managed Services in the field of PeopleSoft Administration and Data Base Administration (DBA) until permanent arrangements are finalized.
3	The UNHCR Division of Information Systems and Telecommunications should implement an integrated service management tool that provides the means to record and monitor all aspects of the agreements entered into with different service providers.	Important	Yes	Deputy Director, Customer Support Service, DIST	Q2 2015	The work-around processes in place will be further reviewed once the new DIST structure is staffed and operational.

---

[6] Critical recommendations address significant and/or pervasive deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance cannot be provided regarding the achievement of control and/or business objectives under review.

[7] Important recommendations address important deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

Management Response

**Audit of the management of externally provided information systems services in the Office of the United Nations
High Commissioner for Refugees**

Rec. no.	Recommendation	Critical[6]/ Important[7]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
4	The UNHCR Division of Information Systems and Telecommunications should review and revoke the administrative rights of all user groups except for the vendor providing the infrastructure services.	Important	Yes	Director, DIST	Q1 2015	Hand over/knowledge transfer to the managed service provider for infrastructure is envisioned to be concluded by Q1 2015. By which time, DIST staff members' administrative access will be revoked.