



INTERNAL AUDIT DIVISION

AUDIT REPORT 2013/028

Audit of the security of the Managing Systems Resources and People (MSRP) system

**Overall results relating to the effective
security management of MSRP were initially
assessed as partially satisfactory.
Implementation of ten important
recommendations remains in progress.**

**FINAL OVERALL RATING: PARTIALLY
SATISFACTORY**

25 March 2013

Assignment No. AT2012/166/01

CONTENTS

	<i>Page</i>
I. BACKGROUND	1
II. OBJECTIVE AND SCOPE	2-3
III. AUDIT RESULTS	4-8
Security of systems and applications supporting the business objectives of the organization	4
IV. ACKNOWLEDGEMENT	9
 ANNEX I Status of audit recommendations	
 APPENDIX 1 Management response	

AUDIT REPORT

Audit of the security of the Managing System Resources and People (MSRP) system

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of the security of the Managing Systems Resources and People (MSRP) system at 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. MSRP is a PeopleSoft/Oracle based enterprise resource planning system and is composed of various functional modules. The human resources (HR) module is managed by the Division of Human Resources Management (DHRM), while the finance and supply chain module is co-managed by the Divisions of Financial and Administrative Management (DFAM) and Emergency Security and Supply (DESS). A software upgrade of MSRP is currently being planned.
4. UNHCR principles of financial accountability and segregation of duties are documented in the financial internal control framework (FICF) of 2006. Their implementation is supported by automated control features available in MSRP for the approval of vouchers, vendors, and purchase orders.
5. In addition, several functions in the expenditure process are segregated by assigning functional roles to individuals in accordance with the operations of UNHCR. Roles are assigned on the basis of a Delegation of Authority Plan (DOAP) and through the use of automated controls, online user access, and system security.
6. Comments provided by UNHCR are incorporated in *italics*.

II. OBJECTIVE AND SCOPE

7. The audit was conducted to assess the adequacy and effectiveness of UNHCR's governance, risk management and control processes in providing reasonable assurance regarding **the effective security management of the MSRP system**.
8. The audit was included in the 2012 OIOS risk-based work plan in consultation with the Division of Information Systems and Telecommunications (DIST). The major risks that led to the selection of this audit included: (a) the departure of key staff members who handled information security functions; and (b) weaknesses in the implementation and monitoring of segregation of duties by the user divisions.
9. The key control tested for the audit was the security of systems and applications supporting the business objectives of the Organization. For the purpose of this audit, OIOS defined this key control as the control that provides reasonable assurance that the security implemented in MSRP addressed the business needs of the Organization.

10. The key control was assessed for the control objectives shown in Table 1.
11. OIOS conducted the audit from 16 August to 31 October 2012. The audit covered the MSRP Human Resources, Finance and Supply Chain modules and the corresponding back-end Oracle databases.
12. 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, 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

13. In OIOS' opinion, the governance, risk management and control processes examined in UNHCR were **partially satisfactory** in providing reasonable assurance regarding **the effective security management of MSRP**. OIOS made ten recommendations to address issues identified in the audit.

14. UNHCR divisions started a series of initiatives to address the risks associated with the security of MSRP. DFAM established processes for identifying role conflicts in the finance module by downloading the user roles in Excel, analyzing them and rectifying the conflicting user roles in MSRP. Given the functional users' limited knowledge of the system, these processes did not ensure a complete identification and resolution of all conflicting roles. DHRM had in place a strict approval process for granting access rights to users. DESS was in the process of revising the related internal control framework.

15. However, the security of MSRP was not adequately controlled and aligned with the changes made in the system since 2006 that included the implementation of other modules like Treasury Management and Human Resources and the rolling-out of MSRP to the country offices.

16. Control weaknesses were also identified with regard to: (i) undefined combinations of conflicting roles; (ii) unavailability of exception reports for the detection of conflicting roles; (iii) undefined and inactive user roles and permissions; (iv) inadequate documentation in support of the establishment of roles in MSRP; and (v) lack of monitoring procedures of users with administrative and superuser privileges. UNHCR was in the process of implementing the relevant recommendations.

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

Table 1: Assessment of key controls

Business objective(s)	Key controls	Control objectives			
		Efficient and effective operations	Accurate financial and operational reporting	Safeguarding of assets	Compliance with mandates, regulations and rules
Effective security management of MSRP	Security of systems and applications supporting the business objectives of the Organization	Partially satisfactory	Partially satisfactory	Partially satisfactory	Partially satisfactory
FINAL OVERALL RATING: PARTIALLY SATISFACTORY					

Security of systems and applications supporting the business objectives of the Organization

Weaknesses in the process of granting and managing roles

18. Roles in the Finance and Supply Chain modules were assigned on the basis of the DOAP. The DOAP was prepared by the representative of a UNHCR country office (or a divisional/regional bureau director at the Headquarters) on an Excel template. The DOAP table was then transmitted to the Financial Control Section (FCS) for approval. FCS reviewed the DOAP and, if found to be correct, confirmed the assigned roles to the users and forwarded it to the MSRP Security Team for recording users and roles in the system. Role changes requested by field offices (additions, deletions and amendments) from previous versions of the DOAP followed the same process. Roles in the HR module were assigned on the basis of ad-hoc requests for authorization, submitted and approved by electronic messages. Once approved, these requests were forwarded to the MSRP Security Team for their recording in the system. However, this process presented the following control weaknesses:

- i. UNHCR did not identify all potential combinations of roles in the system (across modules) that could cause conflicts. MSRP did not have automatic validation controls for preventing the assignment of a conflicting combination of roles (i.e., Preparer and Approver) to the same staff member;
- ii. The types of roles contained in the DOAP were limited to a sub-set of users performing tasks for 'approve spending', 'approve purchase', 'confirm deliver', 'approve payment' and 'execute payment'. Therefore, the DOAP did not regulate roles used by many staff members that access MSRP for performing several other functions (i.e., all HR functions; inventory and asset management functions; and implementing partners management);
- iii. Conflicting roles were assigned to the same staff member in the following instances: Bank Reconciliation Preparer and Approver; Vendor Approver and Voucher Preparer; Requisition Approver and Purchase Order Approver and Goods Receiving; and Implementing Partner Create and Approve;
- iv. FCS created and assigned additional user identification codes (user id) to some staff members (approximately 40) to enable them to perform the 'Voucher Technical Approval' role in addition to their 'Voucher Preparer' role. The assignment of these two roles to the same staff member resulted in having one person preparing and technically approving payment vouchers, thereby defeating one of the main principles of segregation of duties. FCS confirmed that some instances of incompatible roles had to be created in certain country offices because limited staff resources did not allow a complete segregation of duties. However, in these cases, there were no compensating controls in place (i.e., periodic generation of exception reports to confirm that the incompatible roles were only those predefined in the office);
- v. FCS did not review whether the assignment of roles recorded by DIST in MSRP was aligned with the original list of roles approved. Although MSRP provided a report for reviewing the status of the data, this functionality was not used; and
- vi. Some processes were conducted outside MSRP, preventing the detection of potential conflicting roles between the actions performed within and outside MSRP. This was the case for the approval of travel authorizations in country offices. The travel approval process was offline, while payments were online.

(1) The UNHCR Division of Financial and Administrative Management should, in collaboration with the Division of Human Resources Management and the Division of Emergency Security and Supply:

- i. Revisit the FICF/DOAP and produce a comprehensive list of roles in the MSRP system;**
- ii. Define all conflicting combinations of roles across the system and establish validation controls in MSRP to prevent their assignment to a single user;**
- iii. Put in place a mechanism to independently confirm that roles assignment and changes requested are correctly implemented by the Division of Information Systems and Telecommunications; and**
- iv. Design and generate reports on conflicting roles to ascertain their impact and to initiate corrections where necessary.**

UNHCR accepted recommendation 1 and stated that it will initiate a review of the existing system with a view to better define and strengthen the DOAP roles. For this purpose, UNHCR will also take into account the results of the OIOS audit on delegation of authority system in UNHCR which is scheduled to take place in 2013. Implementation of these specific recommendations will be also supported by an eventual upgrade of MSRP. Recommendation 1 remains open pending receipt of documented evidence confirming the establishment of a revised version of the FICF/DOAP, with the identification of conflicting role combinations and the establishment of exception reports to assess the impact of actions performed by users with conflicting roles.

Unused, inactive and undefined roles

19. Over 50 per cent of the 1,110 roles defined in the HR, Finance and Supply Chain modules were not used. Considering the frequent turn-over and mobility of UNHCR staff members across more than 100 duty stations, there was a high risk that some of the inactive roles could be inadvertently assigned to a user, and such assignments could also remain undetected, particularly in light of the weaknesses observed in the DOAP administration. In addition, 289 UNHCR specific roles had no description. Therefore, it was not possible to determine what the purpose of these roles was.

Unused permissions

20. Out of the 2,313 permission lists in the Finance, Supply Chain and HR modules only 994 were used. These unused permissions were not linked to a specific role or process. Some of these inactive permissions could be erroneously assigned to a role and result in potential conflicting duties.

21. UNHCR explained that the proliferation of roles derived from the urgent fixes implemented in the system when MSRP Finance and Supply Chain modules were first deployed to the field offices. During the first period of implementation, users with standard roles experienced difficulties in accessing certain areas of the system and could perform only a part of the designated tasks granted by a standard role. These limitations were addressed by cloning standard roles and then modifying them with the needed credentials. However, after the completion of the deployment and the stabilization of the system, the roles created for addressing the initial limitations were not reviewed and adequately configured.

(2) The UNHCR Division of Information Systems and Telecommunications should assist and support the Divisions of Human Resources, Financial and Administrative Management

and Emergency Security and Supply, to: (i) create an inventory of all roles defined in the system and describe their purpose; and (ii) deactivate roles and permissions that are no longer needed.

UNHCR accepted recommendation 2 and stated that the User Management Section in Amman, with the assistance of the Service Development Section in Budapest, will identify the redundant permissions vis-à-vis the roles and determine the ones which are no longer required and deactivate them. Recommendation 2 remains open pending receipt of documented evidence confirming the establishment of an inventory of all active roles along with their descriptions and related permission lists.

Inadequate documentation supporting the creation of roles

22. DIST did not maintain an adequate record of the documents (approved user requests) supporting the creation of roles and permission lists related to the functions added to MSRP. Also, the mapping of a functional role (example: 'confirm delivery' role), to the corresponding system role(s), was not available in all cases and there was no assurance that it was complete. In addition, the documentation for the roles/permission lists/pages created at the beginning in 2006 was not available for review.

(3) The UNHCR Division of Information Systems and Telecommunications should maintain adequate records of the roles created in MSRP, including details related to permission lists, pages, and corresponding system role(s).

UNHCR accepted recommendation 3 and stated that deactivating redundant permissions and roles (as per recommendation 2) will stabilize and, to a certain extent, address the issue of inadequate documentation in the creation of permissions and roles at the beginning of MSRP implementation stage. As of now, role creation is documented as part of the implementation of any new change request. The relationship of Users, Roles, Permission Lists, Components, Pages, etc., is best documented by on-line queries as it is highly dynamic. Queries will be developed with the assistance of the Service Development Section in Budapest so that these reports can be run on a regular basis and reviewed for consistency. Recommendation 3 remains open pending receipt of the reports documenting the roles created in MSRP, with details of permission lists, pages, and corresponding system roles.

Unmonitored actions of the administrators and superusers

23. Staff members with the role of MSRP system administrator (14), and/or superuser (12), had unlimited access to the system. These roles were assigned to staff members in the technical user group 'MSRP', and other external entities providing IT services to UNHCR (i.e., United Nations International Computing Centre, UNICC). Good practices recommend restricting the number of users with system administrator and superuser roles. Furthermore, to identify/prevent abuse of their privileges, the actions of such users should be monitored. However, DIST had no procedures or reports in place to monitor the actions of the superusers, MSRP system administrators, and the changes made in their roles.

(4) The UNHCR Division of Information Systems and Telecommunications should review the list of MSRP administrators and superusers, reduce their number, and keep the logs of role changes.

UNHCR accepted recommendation 4 and stated that in addition to reviewing and reducing the number of staff members with extended privileges, a review was conducted with UNICC and

appropriate action taken. Furthermore, the ICT Security Officer in DIST will soon put in place procedures and measures to monitor the actions of MSRP superusers and administrators. Recommendation 4 remains open pending receipt of a list of current users with extended privileges in MSRP, and the measures put in place by UNHCR to monitor their actions in the system.

24. There were three users (from a third party service provider) performing development activities in MSRP, who also had access to the production environment (MSRP and Oracle databases). Granting access to both development and production environments to the same user is contrary to industry best practices of segregating access to system environments.

(5) The UNHCR Division of Information Systems and Telecommunications should ensure that system developers do not have access to the production systems.

UNHCR accepted recommendation 5 and stated that it was not a usual practice for developers to be given access to the production system. However, on occasion, this was necessary for support purposes. Control measures would be put in place to ensure that such access is given on a case by case basis to solve specific problems and promptly removed when no longer needed. Recommendation 5 remains open pending receipt of documented evidence demonstrating that access control and monitoring procedures have been put in place for monitoring the activities of the system developers.

Recommended MSRP audit and integrity reports not used

25. MSRP includes audit reports (*DDDAUDIT* - Application Designer/Database Audit Report and *SYSAUDIT* - PS System Table Audit Report) which provide information for checking the integrity of the system, especially after the implementation of major changes (i.e. customization or application of patches). Industry best practices recommend that these reports are run on a regular basis to identify integrity issues, if any, on a proactive basis. In UNHCR, these reports showed a number of exceptions that were shared during the audit field work with the MSRP Security Team in the Information and Communications Technology Services Centre in Amman for further follow-up and action.

(6) The MSRP Security Team in the UNHCR Division of Information Systems and Telecommunications should run the system audit and integrity reports on a regular basis and resolve any exceptions found.

UNHCR accepted recommendation 6 and stated that the MSRP User Administration Team will run the system audit and integrity reports and follow-up on any exceptions found with the assistance of the Service Development Section. Recommendation 6 remains open pending receipt of system audit and integrity reports, and documented evidence of the resolution of any exceptions found.

Security practices not enforced in Oracle databases

26. The following controls were not maintained in accordance with the industry best practices recommended:

- i. An MSRP standard user account ('Outln') remained enabled in the Finance, Supply Chain and HR modules, and the delivered password was not changed. The audit team was able to successfully access the system using the standard credentials. Oracle recommended best practices require a change of password for this account;

- ii. UNHCR still used the ‘System’ account, although best practices recommend disabling it. Furthermore, there was no auditing enabled to monitor the actions of the ‘System’ account. This account was used by UNICC, which also managed its password;
- iii. A user with a powerful account (UNHCR specific database administrator role ‘HCRDBA’) was not monitored with an audit trail that indicated the tasks performed; and
- iv. The passwords associated with Oracle users (about 25 of them) did not expire and had no lockout time or grace time. All the password controls for them were disabled.

(7) The UNHCR Division of Information Systems and Telecommunications should follow the best practices recommended by Oracle for managing powerful accounts related to ‘System’, ‘DBA’ and other delivered accounts, and remove/disable standard credentials.

UNHCR accepted recommendation 7 and stated that system and database administrator (DBA) accounts are managed by the United Nations International Computing Centre (UNICC) to ensure a clear segregation of duties between UNHCR and UNICC. Following UNHCR’s request, the OUTLN account has already been disabled. Recommendation 7 remains open pending receipt of documented evidence confirming the establishment of control mechanisms to monitor powerful accounts in the production system.

Absence of information security policy and need to clarify the role of the Senior Information Security Officer

27. UNHCR has not formulated a comprehensive information security policy. In addition, with the recent establishment of the Senior Information Security Officer’s position in UNHCR, it was unclear whether the responsibilities of the Senior Information Security Officer extended to the security of the application or were limited to the infrastructure only.

(8) UNHCR should formalize a comprehensive information security policy and clarify the responsibilities and role of the Senior Information Security Officer.

UNHCR accepted recommendation 8 and stated that a comprehensive ICT security policy has already been prepared, though yet not finalized, with a copy of the roles and responsibilities of the Senior ICT Security Officer. Recommendation 8 remains open pending receipt of the finalized information security policy.

Change approvals were not logged and documented

28. The review of a sample of system changes showed that adequate documentation existed and that the changes had been tested and approved before they were finally migrated to the production environment. However, the approvals given by the Change Approval Board were not filed correctly. Furthermore, in some cases, the status of the change requests had not been updated in the logs maintained in the LanDesk system.

(9) The UNHCR Division of Information Systems and Telecommunications should ensure that: (i) approvals of changes given by the Change Approval Board are properly filed in a central repository; and (ii) the status of change requests in the logs maintained with the LanDesk system is kept up to date.

UNHCR accepted recommendation 9 and stated that DIST will put in place adequate procedures and control mechanisms so that all changes approved by the Change Approval Board are properly filed in a central repository before they are implemented in the production environment. Currently, the documents are stored in the document management system (Livelink). Recommendation 9 remains open pending receipt of documented evidence confirming the establishment of new procedures for approving and recording changes, with some examples of their implementation.

Hosting services with UNICC

29. The services provided by UNICC to UNHCR for MSRP, including hosting services, were reviewed by an independent consulting firm that issued a Statement on Auditing Standard (SAS) 70 Type II audit report and maturity level in March 2011. The results of this report indicated that some of the controls pertaining to the hosting services provided to clients, such as UNHCR, were in place. However, the tests conducted by OIOS in UNHCR showed that these controls were not functioning as expected, as follows:

Control Assessment per SAS 70 Type II Report	OIOS Assessment
For ERP and mainframe systems, user account management and privileges are managed by the customer.	There were six UNICC users (ICCXX) with PeopleSoft administrator role in MSRP. There was no evidence that the actions of these users were monitored by UNHCR.
The management and strategic direction of information security is reviewed as required at Senior Management Team (SMT) meetings. Specific information security issues are raised regularly at SMT meetings as required.	UNHCR/UNICC had not implemented a number of good practices recommended by Oracle (like locking down user account SYSTEM and enabling of audit trail at the database level).

(10) The UNHCR Division of Information Systems and Telecommunications should review the SAS 70 Type II audit report on UNICC and ensure that all the issues covered in the report that have an impact on UNHCR are addressed.

UNHCR accepted recommendation 10 and stated that DIST will review the SAS 70 report and address any issues relevant to UNHCR. Recommendation 10 remains open pending receipt of documented evidence confirming that actions have been taken for addressing the issues identified in the SAS 70 report.

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.



David Kanja, Assistant Secretary-General
Office of Internal Oversight Services

STATUS OF AUDIT RECOMMENDATIONS

Audit of the security of the Managing System Resources and People (MSRP) System (AT2012/166/01)

Recom. no.	Recommendation	Critical/ ¹ important ²	C/ ³ O ³	Actions needed to close recommendation	Implementation date ⁴
1	<p>The UNHCR Division of Financial and Administrative Management should, in collaboration with the Division of Human Resources Management and the Division of Emergency Security and Supply:</p> <ul style="list-style-type: none"> i. Revisit the FICF/DOAP and produce a comprehensive list of roles in the MSRP system; ii. Define all conflicting combinations of roles across the system and establish validation controls in MSRP to prevent their assignment to a single user; iii. Put in place a mechanism to independently confirm that roles assignment and changes requested are correctly implemented by the Division of Information Systems and Telecommunications; and 	Important	O	Provide documented evidence confirming the establishment of a revised version of the FICF/DOAP, with the identification of conflicting role combinations and the establishment of exception reports to assess the impact of actions performed by users with conflicting roles.	31 Dec 2014

1 Critical recommendations address significant and/or pervasive deficiency or weakness 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.

2 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.

3 C = closed, O = open

4 Date provided by UNHCR in response to recommendations.

Recom. no.	Recommendation	Critical/ ¹ / important ²	C/ O ³	Actions needed to close recommendation	Implementation date ⁴
2	<p>iv. Design and generate reports on conflicting roles to ascertain their impact and to initiate corrections where necessary.</p> <p>The UNHCR Division of Information Systems and Telecommunications should assist and support the Divisions of Human Resources, Financial and Administrative Management and Emergency Security and Supply, to: (i) create an inventory of all roles defined in the system and describe their purpose; and (ii) deactivate roles and permissions that are no longer needed.</p>	Important	O	Provide documented evidence confirming the establishment of an inventory of all active roles along with their descriptions and related permission lists.	30 Jun 2013
3	The UNHCR Division of Information Systems and Telecommunications should maintain adequate records of the roles created in MSRP, including details related to permission lists, pages, and corresponding system role(s).	Important	O	Provide reports documenting the roles created in MSRP, with details of permission lists, pages, and corresponding system roles.	30 Jun 2013
4	The UNHCR Division of Information Systems and Telecommunications should review the list of MSRP administrators and superusers, reduce their number, and keep the logs of role changes.	Important	O	Provide list of current users with extended privileges in MSRP, and the measures put in place by UNHCR to monitor their actions in the system.	30 Jun 2013
5	The UNHCR Division of Information Systems and Telecommunications should ensure that system developers do not have access to the production systems.	Important	O	Provide documented evidence demonstrating that access control and monitoring procedures have been put in place for monitoring the activities of the system developers.	30 Apr 2013
6	The MSRP Security Team in the UNHCR Division of Information Systems and Telecommunications should run the system audit and integrity reports on a regular basis and resolve any exceptions found.	Important	O	Provide system audit and integrity reports, and documented evidence of the resolution of any exceptions found.	30 Apr 2013

Recom. no.	Recommendation	Critical/ ¹ / important ²	C/ O ³	Actions needed to close recommendation	Implementation date ⁴
7	The UNHCR Division of Information Systems and Telecommunications should follow the best practices recommended by Oracle for managing powerful accounts related to 'System', 'DBA' and other delivered accounts, and remove/disable standard credentials.	Important	O	Provide documented evidence confirming the establishment of control mechanisms to monitor powerful accounts in the production system.	30 Jun 2013
8	UNHCR should formalize a comprehensive information security policy and clarify the responsibilities and role of the Senior Information Security Officer.	Important	O	Provide the finalized information security policy.	30 Jun 2013
9	The UNHCR Division of Information Systems and Telecommunications should ensure that: (i) approvals of changes given by the Change Approval Board are properly filed in a central repository; and (ii) the status of change requests in the logs maintained with the LanDesk system is kept up to date.	Important	O	Provide documented evidence confirming the establishment of new procedures for approving and recording changes, with some examples of their implementation.	30 Sep 2013
10	The UNHCR Division of Information Systems and Telecommunications should review the SAS 70 Type II audit report on UNICC and ensure that all the issues covered in the report that have an impact on UNHCR are addressed.	Important	O	Provide documented evidence confirming that actions have been taken for addressing the issues identified in the SAS 70 report.	30 Jun 2013