



OIOS

Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

AUDIT REPORT

UNHCR's information technology security relating to PeopleSoft applications

**UNHCR is yet to establish a comprehensive
information security policy**

17 October 2008

Assignment No. AR2008/166/01

United Nations  Nations Unies

INTEROFFICE MEMORANDUM

MEMORANDUM INTERIEUR

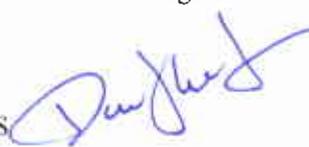
OFFICE OF INTERNAL OVERSIGHT SERVICES BUREAU DES SERVICES DE CONTRÔLE INTERNE
INTERNAL AUDIT DIVISION DIVISION DE L'AUDIT INTERNE

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

DATE 17 October 2008

REFERENCE IAD: 08- 01862

FROM: Dagfinn Knutsen, Director

DE: Internal Audit Division, OIOS 

SUBJECT **Assignment No. AR2008/166/01 - Audit of UNHCR's information technology security relating to**
OBJET **PeopleSoft applications**

1. I am pleased to present the report on the above-mentioned audit.
2. Based on your comments, all the recommendations remain open. In order for us to close the recommendations, we request that you provide us with the additional information as discussed in the text of the report and also summarized in Annex 1.
3. Your response indicated that you did not accept recommendation 14. In OIOS' opinion however, this recommendation seeks to address significant risk areas. We are therefore reiterating it and requesting that you reconsider your initial response based on the additional information provided in the report.
4. Please note that OIOS will report on the progress made to implement its recommendations, particularly those designated as high risk (i.e., recommendations 1, 2, 10, 12, 13, 14 and 16) in its annual report to the General Assembly and semi-annual report to the Secretary-General.

cc: Mr. L. Craig Johnstone, Deputy High Commissioner, UNHCR
Ms. Judy Cheng-Hopkins, Assistant High Commissioner, UNHCR
Ms. Karen Farkas, Controller and Director, DFAM, UNHCR
Ms. Maha Odeima, Audit Coordinator, UNHCR
Mr. Swatantra Goolsarran, Executive Secretary, UN Board of Auditors
Ms. Maria Gomez Troncoso, Officer-in-Charge, Joint Inspection Unit Secretariat
Ms. Christina Post, Administrative Officer, Oversight Support Unit, Department of Management
Mr. Byung-Kun Min, Programme Officer, OIOS
Mr. Anders Hjertstrand, Chief, Geneva Audit Service, OIOS

INTERNAL AUDIT DIVISION

FUNCTION

“The Office shall, in accordance with the relevant provisions of the Financial Regulations and Rules of the United Nations examine, review and appraise the use of financial resources of the United Nations in order to guarantee the implementation of programmes and legislative mandates, ascertain compliance of programme managers with the financial and administrative regulations and rules, as well as with the approved recommendations of external oversight bodies, undertake management audits, reviews and surveys to improve the structure of the Organization and its responsiveness to the requirements of programmes and legislative mandates, and monitor the effectiveness of the systems of internal control of the Organization” (General Assembly Resolution 48/218 B).

CONTACT INFORMATION

DIRECTOR:

Dagfinn Knutsen, Tel: +1.212.963.5650, Fax: +1.212.963.2185,
e-mail: knutsen2@un.org

DEPUTY DIRECTOR:

Fatoumata Ndiaye: Tel: +1.212.963.5648, Fax: +1.212.963.3388,
e-mail: ndiaye@un.org

CHIEF, GENEVA AUDIT SERVICE:

Mr. Anders Hjertstrand: Tel: +41.22.917.2731, Fax: +41.22.917.0011,
e-mail: ahjertstrand@unog.ch

EXECUTIVE SUMMARY

Audit of UNHCR's information technology security relating to PeopleSoft applications

OIOS conducted an audit of UNHCR's information technology security relating to PeopleSoft applications. The audit focused on the security issues relating only to the Management System Renewal Project (MSRP) Finance and Supply Chain Modules. Security of other modules was not reviewed in this audit. The overall objective of the audit was to determine whether security policies existed, were implemented and enforced, and that access to systems and data was restricted to authorized users. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

Most of UNHCR's information technology (IT) security tasks are being discharged by two middle level professional staff members with two assistants. The complex and dynamic tasks for the Security Team were found to be demanding, considering that UNHCR: (a) added important modules like Human Resources/Global Payroll, Budget and Treasury; (b) enhanced the Finance and Supply Chain functionality; and (c) successfully rolled out the Finance and Supply Chain and Budget Modules to over 100 field offices in the recent past. The Security Team nevertheless responded positively to meet these challenges.

UNHCR has yet to formulate a comprehensive information security policy. Staffing restrictions were said to impede the creation of the position of Chief Information Security Officer. Considering the high level of modern information technology in use at UNHCR, it is imperative to protect and safeguard the systems and the data stored therein from misuse or unauthorized use.

OIOS found several weaknesses in the implementation of the Delegation of the Financial Authority Policy (DOAP). These included user accounts that were authorized to perform incompatible roles, and powerful technical user accounts that also had significant business roles. The Division of Financial and Administrative Management (DFAM), as the business owner, should enhance considerably the documentation process, its participation in the granting of access rights to users, and monitoring. This would include establishing new functional roles and permission lists, reviewing the existing ones, and disabling the defunct or redundant ones.

Password management also needed strengthening. Validation controls need to be established in order to prevent the use of obvious strings in passwords. Significant roles assigned to some User IDs related to processing scheduling posed a security risk and needed to be reduced. Requests for programming changes to the MSRP modules need to be categorized by risks.

TABLE OF CONTENTS

Chapter	Paragraphs
I. INTRODUCTION	1 - 6
II. AUDIT OBJECTIVES	7
III. AUDIT SCOPE AND METHODOLOGY	8 - 10
IV. AUDIT FINDINGS AND RECOMMENDATIONS	
A. Security policy and organization	11 - 20
B. Financial Internal Control Framework implementation	21 - 47
C. Oracle database	48 - 54
D. Disaster recovery and business continuity	55 - 59
V. ACKNOWLEDGEMENT	60
ANNEX 1 – Status of Audit Recommendations	

I. INTRODUCTION

1. The Office of Internal Oversight Services (OIOS) conducted an audit of UNHCR's information technology security relating to PeopleSoft applications. The audit focused on security issues relating to the Management System Renewal Project (MSRP) Finance and Supply Chain Modules. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.
2. UNHCR introduced the current web-based PeopleSoft Enterprise Resource Planning (ERP) System known as the MSRP at its Headquarters in 2004. This comprised the Finance and Supply Chain Modules. Subsequently, UNHCR began to roll out MSRP to over 100 field offices. This rollout was completed at the end of 2007. In addition, UNHCR implemented the Budget, Human Resources/Global Payroll and Treasury Modules between 2006 and 2007.
3. UNHCR has a service delivery agreement with the United Nations International Computing Centre (ICC) for hosting its servers for the PeopleSoft applications. This agreement also covers disaster recovery for the production environments.
4. In the middle of 2006, UNHCR revised its delegation of financial authority policy and implemented a new Financial Internal Control Framework (FICF) in the Finance and Supply Chain Modules. This new FICF facilitated more effective financial control while giving the country representatives and senior managers the flexibility to delegate financial authority within their area of responsibility.
5. The MSRP Finance and Supply Chain Modules were enhanced to include the FICF. The FICF was introduced to all offices that went live after 1 July 2006. Offices that went live earlier were brought under the FICF purview later.
6. Comments made by UNHCR are shown in *italics*.

II. AUDIT OBJECTIVES

7. The main objectives of the audit were to determine whether:
 - (a) Security policies and procedures have been issued, implemented and enforced;
 - (b) Access to systems and data is secure and restricted to authorized users based on appropriate identification, authentication and authorization;
 - (c) Controls are in place to ensure that modifications to the system environments are made using a structured process, have appropriate
-

authorizations, are well documented, and are tested before implementation;

(d) Controls exist to ensure the integrity, availability and confidentiality of the data stored in the system;

(e) The technical infrastructure (i.e. servers) supporting the system is secure physically as well as logically; and

(f) Business continuity and disaster recovery plans have been developed, approved, and tested.

III. AUDIT SCOPE AND METHODOLOGY

8. The audit reviewed the controls implemented in the Finance and Supply Chain Modules, and focused mainly on the FICF implementation. In addition, the audit reviewed the critical access controls relating to the back-end database engine of the PeopleSoft application.

9. OIOS assessed the internal controls based on the Information Systems Audit and Control Association's (ISACA) Information Systems Auditing Standards, Guidelines and Procedures and on the relevant processes and control objectives set out in ISACA's Control Objectives for Information and Related Technology (COBIT). OIOS analyzed applicable security data and reviewed available documents and other relevant records. OIOS also observed closely the MSRP Security Team (Security Team) work.

10. The audit did not review the Budget, Human Resources/Global Payroll and Treasury Modules, which are planned to be reviewed separately in the near future.

IV. AUDIT FINDINGS AND RECOMMENDATIONS

A. Security policy and organization

Need for an information security policy and a Chief Information Security Officer

11. UNHCR uses on-line and real-time ERP-based information systems for mission critical functions. In addition, there are other major locally networked applications (like proGres) that are used in the refugee/internally displaced persons' protection and assistance programmes. The security of these systems and the data stored therein is pivotal for accomplishing UNHCR's mission.

12. UNHCR has issued internal memoranda on the FICF, password management, electronic mail and use of computer equipment. However, significant gaps existed in implementing and monitoring these memoranda.

Further, there was no reference to measures that will be taken in the event of non-compliance.

13. Considering UNHCR's high extent of reliance on modern information technology, it is imperative that it has in place a comprehensive information security policy. At the present time, UNHCR has yet to develop such a policy.

14. A proper security policy should specify the functions of the principal information security officer, and the design and implementation of logical access controls covering all resources of the information system. Additionally, the policy should specify the measures that will be taken to enforce compliance.

15. UNHCR's organizational structure does not include the post of a Chief Information Security Officer. The Senior Information Technology Officer who was assigned the handling of security issues was also significantly involved in the roll-out of the PeopleSoft applications to the UNHCR field offices since 2005. With this staff member's departure at the end of September 2007, the post remained vacant until the end of April 2008.

16. UNHCR has in the interim added Human Resources/Payroll and Treasury Modules, enhanced the Finance and Supply Chain Modules and brought over 100 field offices on-line. The surge in the volume of tasks along with the complexity of security issues increased the systems' exposure. Security issues of the PeopleSoft/MSRP applications have been handled by a team of two middle level professional staff with two assistants. OIOS noted that the Security Team successfully discharged their tasks, however overwhelming they have been.

17. OIOS considers that a person who is sufficiently independent of day-to-day IT operations should be designated as Chief Information Security Officer (CISO). The CISO would be responsible for the overall monitoring of compliance with the security policy and procedures. His or her duties would include keeping all security-related documentation up-to-date, performing periodic reviews of the security policy and suggesting changes, performing reviews of the access rights, reviewing security reports, enhancing the security awareness programme for all staff members and informing the Director of the Division of Information Systems and Telecommunications (DIST) of possible threats, any security breaches and unauthorized attempts to access data.

18. DIST appreciated the importance of the comprehensive information security policy and the role of the CISO. However, DIST explained that due to staffing restrictions it was unable to create this post, which has in turn delayed the creation of a formal information security policy.

Recommendations 1 and 2

(1) The UNHCR Division of Information Systems and Telecommunications should, in coordination with the senior management, formulate a comprehensive information security policy to protect UNHCR's information assets.

(2) The Deputy High Commissioner, as Chairperson of the UNHCR Information and Communications Technology Governance Board, should facilitate the creation of the position of the Chief Information Security Officer and define its functions.

19. *The UNHCR Administration accepted recommendation 1 and stated that this was a resource issue and dependent upon the creation of the position of the CISO. Recommendation 1 remains open pending the formulation of a comprehensive information security policy to protect UNHCR's information assets.*

20. *The UNHCR Administration accepted recommendation 2 and stated that the Director (a.i) of DIST has been requested to ensure that the responsibilities of an Information Security Officer are clearly designated to a staff member who has the required competencies. Recommendation 2 remains open pending the creation of the position of CISO and the definition of his/her functions.*

B. Financial Internal Control Framework implementation

Delegation of Financial Authority Policy should be reinforced by comparing the approved Delegation of Financial Authority Policies with their corresponding security profiles

21. The FICF describes the financial functional roles to be performed by a country or field office, and defines the authority and the corresponding system access levels that are needed to perform these functional roles. Each representative/senior manager was required to create a comprehensive Delegation of Financial Authority Policy (DOAP) to implement the FICF. The DOAP provided the mechanism to identify and assign functional roles to staff within their areas of responsibility and to hold them accountable for all actions.

22. The initial DOAP for each field office was established when the MSRP Finance and Supply Chain Modules were rolled out to it. Subsequent modifications (due to staffing or change of function etc) required written/email requests from the representative/senior managers to the Division of Financial and Administrative Management (DFAM). DFAM would review the change request to ensure that there was still sufficient segregation of duties within the office, and that it was otherwise appropriate. If the Security Team found any obvious incongruities in the DOAP (assigning incompatible functional roles for example, which would compromise adequate segregation of duties) and there was no specific indication that these conflicts were acknowledged by DFAM, the Security Team would contact DFAM for clarification before incorporating the changes in the system. The changed version of the DOAP would be provided to DFAM for submission to the representative/senior manager.

23. However, there were weaknesses in the above process. For example, DFAM had not established a process to compare the DOAP data with the data in the MSRP security profiles. In this situation there is no assurance that all the DFAM approved DOAPs (whether initial or subsequently changed versions)

were correctly implemented in the MSRP Finance and Supply Chain Modules. DFAM should therefore review and validate the access privileges that are in effect, and adjust any exceptions. DFAM should also formalize the periodic review and validation of access privileges.

Recommendation 3

(3) The UNHCR Division of Financial and Administrative Management should establish a procedure to compare the approved Delegation of Financial Authority Policy for each cost centre with the corresponding security profile in the Finance and Supply Chain Modules. This comparison should be performed every two months for all the cost centres. Any exception found should be investigated and corrected.

24. *The UNHCR Administration accepted recommendation 3 and stated that an audit query would be developed to report on the security changes and DFAM would use the query to compare changes requested on the DOAP with actual PeopleSoft implementation. Recommendation 3 remains open pending the development of this query and receipt of documentation that it has been fully implemented.*

DOAP should be reinforced by documenting all exceptions to the approved policies

25. There was no assurance that all exceptions to the functional roles specified in the DOAP (which is designed by country offices) were consistently approved by DFAM (the central authority). The audit revealed, and DFAM acknowledged, some conflicting roles in the DOAP MS-Excel sheet which was routinely submitted to the Security Team by electronic mail. However, DFAM had no mechanism in place to detail all the exceptions that had been approved, thus compromising the ability to monitor exceptions. The approval process and the documentation needs to be strengthened.

26. A comparison of the approved DOAPs with the security profiles data in the MSRP Finance and Supply Chain Modules disclosed exception groupings as shown below. The details were shared with the Security Team for corrective action:

- User accounts in the Finance and Supply Chain Modules with assigned functional roles could not be found in the corresponding DOAPs.
- User accounts were provided additional functional roles to those specified in the DOAP.
- Staff members who were in between assignments (SIBAs) had their functional roles attached to their former functions and duty stations though they were no longer there.

-
- User accounts authorized to perform incompatible roles. Examples include: “Bank Reconciliation Preparer” and “Bank Reconciliation Approver”; “Vendor Entry”, “Vendor Certify” and “Vendor Approve”.
 - Powerful technical user accounts (like staff members working in Global Service Desk or MSRP Support) also had significant functional roles and HCR Super User role.
 - A few user accounts had privileges that allowed them to make changes to the production system (migrating objects).
 - In smaller offices where many roles were assumed by a few people, it was necessary for some users to have two User IDs. The secondary User ID was initially created to provide the “Voucher Technical Approval” role. However many (over ninety) ended up having additional roles like “Vendor Approver”, “Vendor Certify” and “Bank Reconciliation Approver”.

Recommendation 4

(4) The UNHCR Division of Financial and Administrative Management should reinforce the process of documenting all the exceptions to the Delegation of the Financial Authority Policy. This process should list the name, date and signature of the approving officer and an explicit confirmation of the conflicting roles a user is authorized to perform.

27. *The UNHCR Administration accepted recommendation 4 and stated that DFAM would reinforce the process and all exceptions would be approved by the Chief, Finance Control Section. Recommendation 4 remains open pending receipt of evidence establishing the process of documenting all exceptions to the DOAP.*

DOAPs should be reinforced by standardizing its content and layout

28. In addition, the layout and contents of the DOAPs were not standardized. Inconsistencies were noted between DOAPs that originated from different country or field offices. For example, the number of columns in the DOAP spreadsheets (representing roles) was not consistent: there were examples of DOAPs that had between 33 and 38 columns. In addition, the DOAPs did not always specify the User IDs, which complicated the comparison of functional roles between the DOAPs and the “Security Profile” data in MSRP.

29. Additionally, while some of the DOAPs contained country-level information, most only contained details relating to a single field office. The DOAPs should also specify the routing-profiles (Country level/Office level permissions) that are assigned to each user, which is not available now.

Recommendation 5

(5) The UNHCR Division of Financial and Administrative Management should standardize the contents and layout of the Delegation of Financial Authority Policy document. There should be one such document for each country. Furthermore, the number of columns in this document should reflect all the functional roles in use and should include the User IDs and their routing-profiles.

30. *The UNHCR Administration accepted recommendation 5 and stated that DFAM would work with DIST to standardize the DOAP document and investigate the delegation of the route control maintenance. Recommendation 5 remains open pending receipt of documentation confirming standardization of the DOAP document.*

Control of access outside the workflow process needs to be standardized and documented

31. There were over 100 assigned functional roles that were not related to any DOAP but provided users with privileges to perform actions and obtain information from the system. Some of these privileges related to Asset Management, Donors and Security Data. While the DOAPs were based on policy, these functional roles were not based on established policy. There was, however, a data protection working group of which DIST was a part.

32. Discussions with the Security Team revealed that non-DOAP related access rights were provided to users upon specific written or email request from the relevant representative or senior manager. Granting such access rights did not always require DFAM approval, though. While there may be no better alternative to this procedure for the time being, OIOS is of the opinion that in this situation there is a significant risk of compromising or diluting the granting of access rights on a strict 'need to know' basis.

Recommendation 6

(6) The UNHCR Division of Financial and Administrative Management and Division of Information Systems and Telecommunications should establish a controlled process of granting access rights to users who do not perform any work flow related tasks under the Delegation of Financial Authority Policy but should nevertheless have access to data and perform certain actions to discharge their work responsibilities.

33. *The UNHCR Administration accepted recommendation 6 and stated that since DFAM was not the exclusive owner of the Finance and Supply Chain Modules, DIST would work with all the business owners and fully document each role and the authorization process that must be followed in order to obtain the role. Recommendation 6 remains open pending receipt of evidence*

establishing the process of granting access rights to users who do not perform work flow related tasks.

Permission lists and roles should be reviewed periodically and processes to create new permission lists and functional roles should be established

34. Permission lists are the building blocks of end user security authorizations. As such, permission lists provide the mechanism by which access to the system is restricted and segregation of duties enforced. Permission lists should be aligned with the business processes and functions to which a specific functional role requires access.

35. Functional roles relate to a function or task and are assigned to users' profiles. Depending on the responsibilities and functions, one or more functional roles can be assigned to a user profile.

36. DFAM, as business owners, should be closely involved in the establishment and review of functional roles and permission lists, an inventory of which should be maintained. However, there is no formal procedure to define and establish functional roles and permission lists which require significant inputs from DFAM. OIOS noted that several functional roles that were customized for UNHCR (HCR prefix) remained unused. Likewise, several of the customized permission lists (HCR prefix) were also not used, and had no User IDs or functional roles attached to them.

37. DFAM should establish a mechanism to determine the active functional roles and the corresponding permission lists. This inventory of functional roles and permission lists should be reviewed periodically by DFAM, who, based on the business needs should create new ones or disable/modify existing ones.

Recommendations 7 to 9

(7) The UNHCR Division of Financial and Administrative Management and the Division of Information Systems and Telecommunications should review and define the various permission lists and functional roles needed for the Management System Renewal Project's Finance and Supply Chain Modules and establish their inventories. Permission lists and functional roles that are not needed for the current business environment but are already included in the security profiles should be disabled.

(8) The UNHCR Division of Financial and Administrative Management and the Division of Information Systems and Telecommunications should establish a formal process to create new permission lists and functional roles in the Management System Renewal Project database.

(9) The UNHCR Division of Financial and Administrative Management and the Division of Information

Systems and Telecommunications should review the permission lists and functional roles in the security profile periodically -- possibly every six months -- to assess their relevance.

38. *The UNHCR Administration accepted recommendations 7, 8 and 9 and stated that since DFAM was not the exclusive owner of the Finance and Supply Chain Modules, DIST would work with all the business owners. New roles and permission lists would be created based on the business requirements of the business owners and would be linked to the change requests. Requests for new roles and permission lists would also be recorded in a database. Recommendation 7 remains open pending receipt of documentation from UNHCR showing that the review of permission lists and functional roles has been undertaken. Recommendation 8 remains open pending receipt of documentation from UNHCR showing that a formal process for the creation of new permission lists and functional roles has been established. Recommendation 9 remains open pending receipt of documentation from UNHCR showing that procedures have been set up to perform periodic reviews of permission lists and functional roles.*

Password management should be reinforced by preventing obvious strings in passwords and raising users' awareness of their obligations and responsibilities

39. UNHCR internal memorandum IOM/FOM 86/2006 dated 28 November 2006 spells out the organization's password policy. The memorandum instructs staff that User IDs and passwords are personal and intended for the protection of both users and information stored in UNHCR's computer systems. Passwords should not be disclosed to anyone under any circumstances. The memorandum also defines what constitutes an improper use of computer resources and establishes personal responsibility and accountability for any losses resulting from the misuse of passwords. Such misuse can be considered misconduct, which may trigger disciplinary proceedings under the Staff Rules. While OIOS appreciates the appropriateness of the password policy, UNHCR should still establish a proper mechanism for monitoring and enforcing compliance with the policy and dealing with exceptions.

40. The following deficiencies in password management were observed:

- Several UNHCR users had easily guessable passwords. OIOS easily managed to decipher about 100 accounts that used such passwords, the details of which have already been shared with the Security Team.
- In some offices many users shared the same password. This could be either due to chance or to an intentional effort to override the separation of duties in the workflow process.
- While it was not possible to recycle recently used passwords, the system nevertheless allowed an unlimited number of password changes during a day, a situation which effectively allowed recycling of passwords.

-
- While procedures were in place to request password resetting, there were some risks. For example, there was no process to compare password reset requests (which are logged in the Global Service Desk database) with the actual logon in the system (a security measure to validate requests for changing/resetting passwords). Neither was there a process to monitor the frequency of password resetting requests. Another example is the possibility to compromise a User ID's access rights by exploiting UNHCR's email system which allows proxy access to users' mail boxes: a proxy user could send an email from the original user account, requesting a password.
 - There was no mechanism to identify and follow-up on: (i) users who frequently changed their passwords; and (ii) users who failed several login attempts.

Recommendations 10 and 11

(10) The UNHCR Division of Information Systems and Telecommunications should prevent the use of obvious strings in passwords and consider increasing the length of the password from the present six characters to eight.

(11) The UNHCR Division of Information Systems and Telecommunications should undertake a programme to raise users' awareness of all information technology related security issues and of users' obligations and responsibilities. Proper emphasis should be placed on warning users of risks associated with providing others with proxy access rights to their own email boxes.

41. *The UNHCR Administration accepted recommendations 10 and 11 and stated that they would be implemented. Recommendation 10 remains open pending receipt of documentation from UNHCR showing that measures have been taken to prevent the use of obvious password strings and that consideration has been given to increasing password length. Recommendation 11 remains open pending receipt of documentation from UNHCR showing that a programme has been initiated to raise users' awareness of their obligations and responsibilities.*

Roles of system process accounts need to be restricted

42. Discussions with DIST officials revealed that one case of suspicious payment was noted last year by a user and was brought to their attention. Though the amount in question was CHF 1 (\$1), DIST referred the case to the Office of the Inspector General for investigation.

43. Currently, there was no procedure in place to identify violations or abuse of access privileges. For example, there were User IDs like AUTOSYS and AUTODBA (for MSRP processing scheduling) whose passwords were known to several users. These user accounts have powerful functional roles like HCR_SUPERUSER, HCR_WEBLIB_EXTRA (AUTOSYS & AUTODBA) and

System Administrator (AUTOSYS). It was not clear whether these functional roles were essential to these accounts. Violations or abuse of these accounts would be difficult to identify.

44. In OIOS' view, consideration should be given to curtailing the functional roles assigned to AUTOSYS and AUTODBA user accounts, or alternatively assigning their current privileges to individual users and locking these user accounts. With the shared password currently in effect, the responsibility for the actions of these account holders cannot be definitely established.

Recommendation 12

(12) The UNHCR Division of Information Systems and Telecommunications should restrict the functional roles assigned to AUTOSYS and AUTODBA user accounts. If not needed, these user accounts should be locked and their privileges reassigned to individual user accounts.

45. *The UNHCR Administration accepted recommendation 12 and stated that DIST has already started the process of removing the functional roles from the AUTOSYS users account and user accounts similar to AUTOSYS and these efforts would continue. Since these user accounts are needed in the operations they would not be discontinued.* Recommendation 12 remains open pending receipt of documentation from UNHCR showing that roles of system process accounts have been restricted.

Incident response procedures should be established

46. There were no predefined scenarios which would constitute high-risk events, and would therefore trigger automated issuance of alerts to the security administrators. Neither were there established procedures for responding to such events. An example of such a scenario would be the use of the AUTOSYS account to post a journal entry to the General Ledger (the AUTOSYS account is normally not assigned to business users; it is used for system maintenance tasks). Indeed, in a recently concluded OIOS audit of a UNHCR field office, this exact scenario was used to conceal a fraudulent, long-time pending transaction. Although in that case a breakdown in accounting controls was also involved, the posting of transactions through unusual user accounts an exception that should be reported and investigated further.

Recommendation 13

(13) The UNHCR Division of Information Systems and Telecommunications in cooperation with the Division of Financial and Administrative Management should identify scenarios that constitute high risk events and establish reporting procedures to identify them for further investigation and follow-up.

47. *The UNHCR Administration has not commented upon this recommendation. Recommendation 13 remains open pending receipt of documentation from UNHCR showing that procedures have been established to identify high risk events and report on them.*

C. Oracle database

Risks of using delivered accounts with delivered and shared passwords

48. OIOS' review of the user accounts in the Finance and Supply Chain (Production and Pre-production) databases revealed that the "Oracle" delivered accounts like SYSTEM, SYS and DBSNMP remained enabled. Good security practices required that these accounts should be expired and locked out and that their default (delivered) passwords changed. However, since the privileges assigned to these accounts are essential for the functioning of the system, the privileges should be reassigned to individual accounts.

49. The passwords for the SYS and SYSTEM accounts were changed, but that the database administrators at DIST and at ICC (the hosting services provider) knew (shared) them. Additionally, as part of its audit tests, OIOS successfully logged in using the DBSNMP account (which had privileges to create new tables, for example, in the database) and the delivered password which had not been changed. This test result was brought to the attention of DIST, who acted to correct it.

50. DIST should give consideration to expiring and locking out all the "Oracle"-delivered accounts, in particular the powerful SYS and SYSTEM accounts. With a shared password, the responsibility for actions of these accounts cannot be established with any certainty at present.

Recommendation 14

(14) The UNHCR Division of Information Systems and Telecommunications should expire and lock out all the delivered accounts, in particular the powerful SYS and SYSTEM accounts, and reassign their corresponding privileges to individual user accounts.

51. *The UNHCR Administration did not accept recommendation 14, stating that the two delivered accounts SYS and SYSTEM were needed and would not be disabled. DIST would institute a regular password change policy with ICC that would strictly limit who has access to the passwords for these accounts, mandate regularly scheduled changes to the passwords for these accounts, and would also mandate a change to the passwords for these accounts anytime someone on the MSRP team at ICC left ICC employment. Furthermore, these user accounts were controlled by the ICC and only a very small number of ICC employees have knowledge of the password for these accounts while no one from UNHCR has such knowledge. The SYS and SYSTEM accounts were used to start databases, backup databases, and similar database related activities. These accounts were not used to run SQL updates to the production databases. OIOS takes note of the*

explanations provided by UNHCR and will leave recommendation 14 open pending the issuance of a documented password change policy, and evidence that measures have been put in place to control who has access to the password of SYS & SYSTEM accounts.

Change management requests should be categorized based on risks

52. UNHCR uses the following computer environments for the MSRP system life cycle: “Development”, “User Acceptance Test”, “Pre-Production” and “Production”. DIST explained that ICC was responsible for migrating changes to the “Pre-production” and “Production” environments. OIOS reviewed a sample of change requests for migration and was satisfied with the signoff process.

53. DIST maintained a Microsoft Access-based database called “Request Management System” to record the change requests for all the UNHCR information system applications and databases. However, there was no easy means of categorizing the changes requested: by nature (i.e., changes to PeopleCode, new reports, changes to existing pages etc.) Furthermore, change requests were not marked by risks and by their potential impact on the Production Environment.

Recommendation 15

(15) The UNHCR Division of Information Systems and Telecommunications should categorize the change requests (example: PeopleCode, new table, new field), assess and record their risks and the potential impact on the Production Environment.

54. *The UNHCR Administration accepted recommendation 15 and stated that DIST was in the process of developing a Change Management module in the MSRP Portal that would be used to track changes to all the MSRP systems. Categorization of changes and an area for risk assessment would be included in the development of the new module. Recommendation 15 remains open pending receipt of documentation from UNHCR showing that the change management module has been implemented.*

D. Disaster recovery and business continuity

Successful disaster recovery tests by UNHCR

55. The ICC service delivery agreement with UNHCR for the hosting services covers disaster recovery for the production environments of the MSRP’s Finance and Supply Chain, Human Resources/Payroll, Budget and Portal Modules. This agreement mitigates risks of fire, flooding, plane crash and denied access to UNHCR’s primary site. The disaster recovery centre is located in Geneva with a recovery time objective of 24 hours and a recovery point objective of four hours from the declaration of a disaster. The disaster server

infrastructure will have a 50 per cent capacity of normal production but will have the capability to scale to normal (100%) level at short notice.

56. DIST explained that the disaster recovery site was tested in phases during June and July 2008. These were the first tests since Human Resources /Payroll and Treasury Modules were added to the ERP. *DIST explained that the disaster recovery testing of the MSRP systems with ICC in July 2008 were successful.*

Business continuity plan should be updated

57. Business continuity planning is designed to reduce UNHCR's risk of an unexpected disruption of its critical functions and assure continuity of a minimal level of services necessary for critical business operations. The plan should address all functions and assets required for UNHCR to continue as a viable organization. This would include all types of events that have an impact on critical information systems, processing facilities and user business functions.

58. DIST explained that a business continuity plan was prepared several years ago to address the Avian Influenza Pandemic scenario. DIST acknowledged that this plan should be revised/updated as UNHCR in the recent past has outposted some of its mission critical departments like Finance, Human Resources and Supply Chain Management to Budapest, Hungary. Furthermore, the High Commissioner's Decision on Outposting (IOM 042/2007 FOM 045/2007) dated 12 June 2007 had assigned the business continuity plan to the Implementation Task Force chaired by the Deputy High Commissioner. However, the current status of this plan is unclear.

Recommendation 16

(16) The Deputy High Commissioner, as Chairperson of the UNHCR Outposting Implementation Task Force, should initiate action to update the business continuity plan for UNHCR.

59. *The UNHCR Administration accepted recommendation 16 and stated that the Deputy High Commissioner initiated discussions on a business continuity plan for UNHCR in April 2008 and requested the Division of Operations Support (DOS) to lead the process for the development of such a plan. An initial concept paper was developed by DOS and a proposal would be drafted in the near future. Recommendation 16 remains open pending receipt of documentation from UNHCR showing that the business continuity plan has been updated.*

V. ACKNOWLEDGEMENT

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

STATUS OF AUDIT RECOMMENDATIONS

Recom. no.	Recommendation	Risk category	Risk rating	C/O	Actions needed to close recommendation	Implementation date ²
1	The UNHCR Division of Information Systems and Telecommunications should, in coordination with the senior management, formulate a comprehensive information security policy to protect UNHCR's information assets.	Governance	High	O	Documentation for the formulation of a comprehensive information security policy to protect UNHCR's information assets.	Not provided.
2	The Deputy High Commissioner, as Chairperson of the UNHCR Information and Communications Technology and Governance Board, should facilitate the creation of the position of the Chief Information Security Officer and define its functions.	Governance	High	O	Creation of the position of the Chief Information Security Officer and his/her functions are defined.	Not provided.
3	The UNHCR Division of Financial and Administrative Management should establish a procedure to compare the approved Delegation of Financial Authority Policy for each cost centre with the corresponding security profile in the Finance and Supply Chain Modules. This comparison should be performed every two months for all the cost centres. Any exception found should be investigated and corrected.	Operational	Medium	O	The development of this query and receipt of documentation that it has been fully implemented.	31 Dec 2008
4	The UNHCR Division of Financial and Administrative Management should reinforce the process of documenting all the exceptions to the Delegation of the Financial Authority Policy. This process should list the name, date and signature of the approving officer and an explicit confirmation of the conflicting roles a user	Operational	Medium	O	Receipt of evidence establishing the process of documenting all exceptions to the Delegation of Financial Authority Policy.	31 Dec 2008

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
5	is authorized to perform. The UNHCR Division of Financial and Administrative Management should standardize the contents and layout of the Delegation of Financial Authority Policy document. There should be one such document for each country. Furthermore, the number of columns in this document should reflect all the functional roles in use and should include the User IDs and their routing-profiles.	Operational	Medium	O	Receipt of documentation confirming standardization of the Delegation of Financial Authority Policy document.	30 Sep 2009
6	The UNHCR Division of Financial and Administrative Management and Division of Information Systems and Telecommunications should establish a controlled process of granting access rights to users who do not perform any work flow related tasks (under the Delegation of Financial Authority Policy) but should nevertheless have access to data and perform certain actions to discharge their work responsibilities.	Operational	Medium	O	Receipt of evidence establishing the process of granting access rights to users who do not perform work flow related tasks.	30 Sep 2009
7	The UNHCR Division of Financial and Administrative Management and the Division of Information Systems and Telecommunications should review and define the various permission lists and functional roles needed for the Management System Renewal Project's Finance and Supply Chain Modules and establish their inventories. Permission lists and functional roles that are not needed for the current business environment but are already included in the security profiles should be disabled.	Operational	Medium	O	Receipt of documentation from UNHCR showing that the review of permission lists and functional roles has been undertaken.	30 Sep 2009
8	The UNHCR Division of Financial and Administrative Management and the	Operational	Medium	O	Receipt of documentation from UNHCR showing that a formal process for the	31 Dec 2008

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
9	<p>Division of Information Systems and Telecommunications should establish a formal process to create new permission lists and functional roles in the Management System Renewal Project database.</p> <p>The UNHCR Division of Financial and Administrative Management and the Division of Information Systems and Telecommunications should review the permission lists and functional roles in the security profile periodically - possibly every six months - to assess their relevance.</p>	Operational	Medium	O	<p>creation of new permission lists and functional roles has been created.</p> <p>Receipt of documentation from UNHCR showing that procedures have been set up to perform periodic reviews of permission lists and functional roles.</p>	30 Sep 2009
10	<p>The UNHCR Division of Information Systems and Telecommunications should prevent the use of obvious strings in passwords and consider increasing the length of the password from the present six characters to eight.</p>	Operational	High	O	<p>Receipt of documentation from UNHCR showing that measures have been taken to prevent the use of obvious password strings and that consideration has been given to increasing password length.</p>	31 Dec 2008
11	<p>The UNHCR Division of Information Systems and Telecommunications should undertake a programme to raise users' awareness of all information technology related security issues and of users' obligations and responsibilities. Proper emphasis should be placed on warning users of risks associated with providing others with proxy access rights to their own email boxes.</p>	Operational	Medium	O	<p>Receipt of documentation from UNHCR showing a programme has been initiated to raise users' awareness of their obligations and responsibilities.</p>	31 Dec 2008
12	<p>The UNHCR Division of Information Systems and Telecommunications should restrict the functional roles assigned to AUTOSYS and AUTODBA user accounts. If not needed, these user accounts should be locked and their privileges reassigned to individual user accounts.</p>	Operational	High	O	<p>Receipt of documentation from UNHCR showing that roles of system process accounts have been restricted.</p>	31 Dec 2008

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
13	The UNHCR Division of Information Systems and Telecommunications in cooperation with the Division of Financial and Administrative Management should identify scenarios that constitute high risk events and establish reporting procedures to identify them for further investigation and follow-up.	Operational	High	O	Receipt of documentation from UNHCR showing that procedures have been established to identify high risk events and report on them.	Not provided.
14	The UNHCR Division of Information Systems and Telecommunications should expire and lock out all the delivered accounts, in particular the powerful SYS and SYSTEM accounts, and reassign their corresponding privileges to individual user accounts.	Operational	High	O	Issuance of a documented password change policy and evidence that measures have been put in place to control who has access to the password of SYS and SYSTEM accounts.	Not provided
15	The UNHCR Division of Information Systems and Telecommunications should categorize the change requests (example: PeopleCode, new table, new field), assess and record their risks and the potential impact on the Production Environment.	Operational	Medium	O	Receipt of documentation from UNHCR showing that the change management module has been implemented.	30 Sep 2009
16	The Deputy High Commissioner, as Chairperson of the UNHCR Outposting Implementation Task Force, should initiate action to update the business continuity plan for UNHCR.	Strategy	High	O	Receipt of documentation from UNHCR showing that the business continuity plan has been updated.	Not provided.

1. C = closed, O = open
2. Date provided by UNHCR in response to recommendations.