



UNITED NATIONS

NATIONS UNIES

INTERNAL AUDIT DIVISION I
OFFICE OF INTERNAL OVERSIGHT SERVICES

Reference: AUD-7-1:6 (0305 /05)

23 May 2005

To: Ms. Rosemary McCreery, Assistant Secretary-General
for Human Resources Management

From: Patricia Azarias, Director
Internal Audit Division I, OIOS

A handwritten signature in black ink that reads "P. Azarias".

Subject: **OIOS Audit No. AH2004/512/04 (formerly AH2004/512/02B): Review of OHRM Information and Communications Technology Management**

1. I am pleased to present herewith our final report on the subject audit. I would like to thank you for the comments that you sent us in your communication dated 5 May 2005 in response to our draft report of 2 February 2005. We have included your comments in the report after the respective recommendation.
2. I would appreciate if you could provide me with an update on the status of implementation of the audit recommendations not later than 30 November 2005. This will facilitate the preparation of the twice-yearly report to the Secretary-General on the implementation of recommendations, required by General Assembly resolution 48/218B.
3. I would like to thank you and your staff for the assistance and co-operation provided to the auditor.

Copies to:

Ms. J. Beagle
Ms. Sandra Haji-Ahmed
UN Board of Auditors
Programme Officer, OIOS



United Nations
OFFICE OF INTERNAL OVERSIGHT SERVICES
Internal Audit Division I

AUDIT REPORT

Audit subject: Review of OHRM Information and Communications
Technology Management
Audit No.: AH2004/512/02B
Report date: 23 May 2005
Audit team: Leonard Gauci, Auditor-in-Charge

OIOS review of OHRM ICT Management

Executive Summary

This review was conducted in parallel with an ICT audit of the Galaxy system. OIOS focused on the areas of ICT policy and strategy, criteria for the selection of application systems, technical support to users and plans for business continuity in the event of a major disaster affecting IT systems.

OIOS was presented with a draft document titled "Human Resources Information and Communication Technology Strategy". This was compiled between June 2001 and April 2003. The document was not approved at the Assistant Secretary-General level and requires updating to accommodate developments that have taken place during the past two years. The ICT strategy needs to define governance as well as ownership of systems and data. It also needs to be more specific on the personnel and financial resources required to achieve the strategic objectives. Without a proper analysis and definition of these aspects it will be difficult to apply the strategy in practice. The ICT strategy should be aligned with the global ICT strategy of the Secretariat. Once the strategy document has been updated, it should be approved by OHRM's ICT Steering Committee and the ICT Committee of the Department of Management.

All proposed application systems should be subject to an evaluation between in-house development, sub-contracting and a vendor package solution, and submitted to the Project Review Committee of the Secretariat's Information and Communications Technology Board for review. All software development agreements should include criteria for systems delivery and user acceptance.

There are no Service Delivery Agreements covering the ICT services provided to OHRM or the services that OHRM provides to the users of its systems. OHRM should take steps so that both ICT services as well as the respective responsibilities of the parties concerned are defined in such agreements.

OHRM should take the lead in launching a review of all operating and user procedures for its application systems, and to draw up an updated training programme for users of application systems such as IMIS and Galaxy.

The Office should ensure that the work being undertaken by the Information Technology Services Division on ICT security and business continuity is extended to cover the ICT environment and core applications that fall under its responsibility.

TABLE OF CONTENTS

Chapter	Paragraphs
I. INTRODUCTION	1
II. AUDIT SCOPE, OBJECTIVES AND METHODOLOGY	2 – 4
III. FINDINGS AND RECOMMENDATIONS	5 – 25
A. ICT Strategy and Policy issues at the OHRM level	5 – 10
B. Selection, development and implementation of systems	11 – 13
C. Technical support and ICT services	14 – 17
D. User procedures, training and support	18 – 20
E. ICT Security and Business Continuity	21 – 25
IV. ACKNOWLEDGEMENT	26

I. INTRODUCTION

1. The review was carried out between April and September 2004 at the United Nations Headquarters in New York in accordance with the International Standards for the Professional Practice of Internal Auditing, promulgated by the Institute of Internal Auditors and adopted by the Internal Audit Services of the United Nations Organizations.

II. AUDIT SCOPE, OBJECTIVES AND METHODOLOGY

2. The review was conducted parallel to an ICT audit of the e-staffing system and Galaxy project that OIOS was performing at the Operational Services Division. It did not examine the IT controls over individual application systems or the functionality aspects of systems implemented within OHRM.

3. The main objectives of the audit were to evaluate the adequacy and effectiveness of procedures to ensure:

- Proper governance over ICT, a well-defined ICT strategy which supports the mandate of the Office and is backed by adequate budgeting and funding, and an appropriate ICT organizational structure and resources;
- The use of appropriate systems architecture, technology and application systems, appropriate procedures over the selection, development and implementation of systems and change control procedures;
- The provision of technical support to ensure a continued and efficient service to users; and
- Adequate policies for ICT security and business continuity planning.

4. The review was based on a series of questionnaires and interviews with key personnel involved in the information and communications technology function. OIOS also reviewed supporting documentation and current practices relevant to the audit objectives.

III. FINDINGS AND RECOMMENDATIONS

A. ICT Strategy and Policy for OHRM

5. The Divisions within OHRM that have significant standalone IT products and services are OSD, the Division for Organizational Development and the Medical Services Division.

6. OHRM/OSD does not have an updated information technology systems strategy that is approved at the ASG level and endorsed by the ICT Committee of the Department of Management. OIOS was presented with a copy of a document titled "Human

Resources Information and Communication Technology Strategy”. This document defines the methodology by which OHRM should use technology to improve its effectiveness and services. It was compiled between June 2001 and April 2003. At the time of audit, the draft document was for the review of the ASG, OHRM.

7. Among the priorities identified in the strategy document that have been addressed is the setting up of an HR-ICT Steering Committee. This committee, chaired by the ASG for Human Resources Management, has as members the three D2 directors of OHRM, and the Chief HRITS who also acts as secretary. This Committee is responsible for seeing that the HR-ICT strategy is being followed. However, there is also an ICT Committee for the Department of Management set up in line with the requirements of the Secretary-General’s bulletin on “Information and Communications Technology Board”¹, of which the Director of OSD and the Chief of HRITS are members.

8. OIOS agrees that “HR technology support staff should reside with and report into OHRM, with a direct link to ITSD”² and also notes that as one of the keys to success, the strategy identifies the support and involvement of ITSD in a “partnership effort”³. However, the document does not define governance and the ownership of software and data. The strategy also needs to be more specific about resources, both human and financial. In paragraph 4.3.1 it states “The new model requires full-time, dedicated HR technology support staff with skills in data and systems analysis, programming (particularly Web development tools), and reporting. *The exact number of people will depend on the extent of technologies and applications implemented and in development, as well as budget restrictions*” (OIOS italics).

9. The report needs to be more specific on the measures that are necessary to turn the strategy into a reality. This should be the role of the HR-ICT Steering Committee, which should also provide a strong monitoring function to immediately identify where things are not going to plan, take corrective measures, and amend the strategy as appropriate.

10. The ICT strategy should be a workable one with clearly identified priorities, resources and concrete deliverables in a realistic time schedule. The strategy may also need to be modified as a result of changes to the mandate and policies of OHRM and the Committee must ensure that these changes will not be delayed because of lack of preparedness in the ICT infrastructure of the Office. There should also be adequate structures to ensure that the ICT strategy and policy are at all times aligned with those of the Secretariat.

Recommendation 1

OHRM should provide an updated HR ICT strategy for the approval of the OHRM ICT Steering Committee and present

¹ ST/SGB/2003/17 para. 4.4

² Human Resources Information and Communication Technology Strategy – Draft para. 4.3.1

³ *ibid.* para. 4.5

it to the ICT Committee of the Department of Management for its endorsement (AH2004/512//02B/01).

Management response: *Accepted for implementation in the third quarter of 2005.*

OIOS takes note of management's response. It will keep this recommendation open pending receipt of the approved HR ICT strategy.

Recommendation 2

The OHRM ICT Steering Committee should have a mechanism to ensure that the ICT strategy is adhered to in practice, remains up-to-date with the mandate and policies of the Office, and is aligned with the global ICT strategy of the Secretariat (AH2004/512/02B/02).

Management response: *Accepted.*

OIOS will close this recommendation when it receives documentation outlining the measures implemented by the OHRM ICT Steering Committee to ensure compliance with the strategy, and keeping it up-to-date and aligned with that of the Secretariat.

B. Selection, development and implementation of systems

11. The revised information and communications technology strategy for the Secretariat worldwide identifies the statement on return on investment as the primary determining factor in assigning priorities to ICT projects and initiatives. It includes the use of mandatory cost-benefit analyses as a prerequisite for the development of all new systems and for the initiation of ICT-related projects to ensure a consistent approach and returns on investment⁴. The General Assembly also requested the Secretary-General to provide a mechanism to assess the rationale for investment.⁵ OIOS noted that the draft ICT strategy document for OHRM stipulates that a business case must be made to obtain funding for the development of new systems⁶.

12. The Secretary-General's bulletin "Information and Communications Technology Board" established a Project Review Committee "to apply uniformly the standards decided upon by the Information and Communications Technology Board to information and communications technology initiatives within the Organization and to recommend whether such initiatives should proceed."⁷ This Committee is to review proposed ICT projects to justify the rationale behind the investment, ensure that the total cost of projects is accurately projected, standard development methodologies are applied and all relevant documentation is available.

⁴ A/57/620 para. 77

⁵ Resolution 57/304 of 15 April 2003, paragraph 4

⁶ Human Resources Information and Communication Technology Strategy – Draft para. 5.1

⁷ ST/SGB/2003/17 para. 5.2

13. Galaxy was planned and developed before the above requirements came into being. However, for all future software selection or development projects, OHRM should follow the procedures set by the Secretariat's Information and Communications Technology Board, including the presentation of new initiatives before the Project Review Committee. The submissions should be backed by a business case and presented following an evaluation of the options of software development and the purchase of an ERP package. There should also be criteria defining the point at which a software development project is completed and the point at which the service by the contractor becomes one of support and maintenance.

Recommendation 3

OHRM should not develop or commission any new application systems until its ICT strategy is adopted and criteria for systems selection and development, including return on investment, where feasible, are set (AH2004/512/02B/03).

Recommendation 4

The OHRM ICT Steering Committee should see that:

- (a) No new project is approved without a preliminary evaluation that includes its financial impact;
- (b) A comparative analysis of purchasing a package system against developing it in-house, or subcontracting it, be made mandatory for all proposed systems; and
- (c) All agreements regarding software development and systems implementation clearly define the acceptance criteria and the point of delivery of the system (AH2004/512/02B/04).

Management response for recommendations 3 and 4: *Accepted for new products except for those in the pipeline.*

OIOS takes note of management's response. OIOS appreciates that applying recommendations 3 and 4 retrospectively may not be practical, and accordingly, directed these recommendations to new systems and new projects. It would appreciate a clarification from management of the term "in the pipeline" and a list of products that fall under this heading. OIOS will keep this recommendation open pending management's further reply.

C. Technical support and ICT services

14. The Department of Management's Information Technology Services Division currently provides desktop support and CMS on a head-count level as well as network support to OHRM personnel. These arrangements are not formalized and do not cover the on-going support of application software developed in-house such as IMIS.

15. OIOS is of the opinion that a formal agreement between OHRM and ITSD defining the services to be provided by the latter and the responsibilities of both parties would be beneficial to users, avoid misunderstandings and in line with best practice.

16. Such an agreement would describe the services ITSD would provide to OHRM in terms of networks, user support and Help Desk, detail the responsibilities of each party and set performance guidelines. It should include support for application software that is supported by ITSD. In addition to IMIS, this would include Galaxy once the development and support functions have been migrated from DPKO. It would also specify those areas where support is not provided. The agreement would include information on any cost that ITSD charges to OHRM (e.g. per workstation per annum).

17. The ICT services provided by OHRM, for example through OSD to users of Galaxy in UN departments and Offices, are not clearly defined and agreed upon in a Service Level Agreement (SLA). OHRM should also take steps to draw up and have its clients sign SLAs.

Recommendation 5

OHRM should carry out an exercise to identify all those ICT services that are being provided by the Department of Management's Information Technology Services Division, and together with ITSD have these services and respective responsibilities defined in a Service Level Agreement signed by both parties (AH2004/512/02B/05).

Management response: *Accepted for implementation in the 3rd quarter 2005.*

OIOS takes note of management's response. It will close this recommendation once it receives a copy of the Service Level Agreement signed by OHRM and ITSD.

Recommendation 6

OHRM should formalize the ICT services that are being provided to users in a Service Level Agreement signed by both parties (AH2004/512/02B/06).

Management response: Management response: *Accepted for implementation in the 4th quarter 2005.*

OIOS takes note of management's response. It will close this recommendation once it receives a copy of the Service Level Agreements.

D. User procedures, training and support

18. Procedures covering the day-to-day use of application systems, and their management and control should be available and kept in line with systems development. ITSD is responsible for providing procedures related to the Local Area Network and

desktop support. The development and maintenance of user procedures related to the application is the responsibility of the application owner. Current operating and user procedures need to be updated and standardized.

19. While up-to-date user and operating procedures are required for the effective and efficient use of all systems and resources, new users of core application systems such as IMIS and Galaxy also need proper training to help them use the system features to best effect. In the case of Galaxy, new enhancements and modules are being rolled out and the system owners are responsible for providing training to users in the day-to-day operation of systems, their management and control.

20. OIOS noted that training in Galaxy has not been provided on a regular basis, possibly because resources were assigned to other more urgent tasks. In the case of IMIS, training needs to undergo a thorough review to bring it in line with the latest system version and incorporate any lessons learnt.

Recommendation 7

The Operational Services Division, in coordination with DPKO and ITSD should review all operating and user procedures for core application systems such as IMIS and Galaxy with a view to update and standardize them (AH2004/512/02B/07).

Management response: *Accepted, already in progress.*

OIOS takes note of management's response. It will close this recommendation once it receives a copy of the updated operating and user procedures.

Recommendation 8

The Operational Services Division should liaise with DPKO, ITSD and the Staff Development Division of OHRM to identify resources and draw up an updated training programme for users of core application systems such as Galaxy and IMIS (AH2004/512/02B/08).

Management response: *While OHRM accepts this recommendation, it is important to note that the drawing up of training programmes is dependent on fulfilling Recommendation 7. IMIS and Galaxy are systems in need of major revisions and standardization especially in terms of efficient workflows, connectivity, and usability. In principle, only applications that meet current ICT standards, and have service level agreements can be supported by the Staff Development Service. Otherwise, those systems must continue to rely on the training already developed and currently in place.*

OIOS takes note of management's response. It agrees that the implementation of this recommendation is dependent on recommendation 7 (as well as recommendation 6). Management stated that recommendation 6 would be implemented by the end of 2005

while implementation of recommendation 7 is in progress. OIOS suggests that management set target dates for implementing this recommendation and will keep the recommendation open pending the receipt of an updated training programme for users of the core systems.

E. ICT Security and Business Continuity

21. OHRM does not have a documented security policy covering its applications or a Business Continuity Plan aimed at ensuring that in the event of a disaster it will continue to provide its core services effectively while properly restoring the facilities.

22. In its report following a post-implementation review of IMIS⁸, OIOS had recommended that ITSD follow up on the Board of Auditors' recommendations for undertaking an information systems risk analysis and the implementation of an information systems security policy.⁹ ITSD said it has already completed four ICT Security Risk Assessments (NYHQ/LAN & MAN, UNON, ECA and ECLAC) and planned to complete assessments for all OAHs by the end of 2004. However, these Security Risk Assessments do not cover Galaxy as yet.

23. In the same report on IMIS, OIOS had recommended that ITSD take the lead in developing and implementing a comprehensive Business Continuity Plan¹⁰. ITSD has informed OIOS that the ICT Security and Business Continuity Policy is under review for completion by the end of 2004. ITSD said that in addition, it has initiated the preparation of an ISO17799 information security compliance project that will define and regulate procedures for system failures and disaster recovery within a comprehensive ICT security framework and that Business Continuity will be addressed under this project. Proposals being formulated by ITSD for Global Business Continuity also recognize the significant business impact of non-availability of IMIS.

24. ICT Security and Business Continuity call for careful and thorough planning, and require significant allocation of funds and staff. They also require coordination between several parties such as the suppliers of hardware, software and communications equipment. DPKO has already undertaken and consolidated planning related to Business Continuity, utilizing its headquarters in New York, the UN Logistics Base in Brindisi and the United Nations office in Geneva as disaster recovery sites.

25. The Galaxy system is related to IMIS and there is the proposed migration of Galaxy programming and support tasks from DPKO to ITSD. OHRM should seek to benefit from the work already undertaken by ITSD and DPKO in this area and actively participate to ensure that the ICT Security and Business Continuity Planning adequately cover those applications for which it is responsible.

⁸ AM/2001/54/1

⁹ AM2001/54/25

¹⁰ AM2001/54/29

Recommendation 9

OHRM should request the Department of Management's Information Technology Services Division to include Galaxy and other core application systems of which it is the owner in its ICT Security Risk Assessments (AH2004/512/02B/09).

Management response: *Accepted, already in progress.*

OIOS takes note of management's response. It will close this recommendation once it receives a copy of the relevant ICT Security Risk Assessment.

Recommendation 10

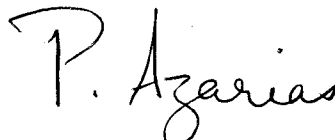
OHRM should actively participate and seek to benefit from the work already undertaken by ITSD and DPKO related to Business Continuity Planning and ensure that the applications for which it is responsible are adequately covered in such plans (AH2004/512/02B/10).

Management response: Management response: *Accepted for implementation in 2005-2006 subject to ITSD capacity.*

OIOS takes note of management's response. It will close this recommendation once it receives a copy of the relevant business continuity plans.

IV. ACKNOWLEDGEMENT

26. We wish to express our appreciation for the assistance and cooperation extended to the auditors.



Patricia Azarias, Director
Internal Audit Division I/OIOS