INTERNAL AUDIT DIVISION

AUDIT REPORT

Information and communications technology governance and security management in UNMIS

Unmitigated risks in the governance of ICT resources and the security of ICT operations need to be addressed

11 December 2009
Assignment No. AT2008/632/01

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. Ashraf Jehangir Qazi, DATE: 11 December 2009
A: Special Representative of the Secretary-General
United Nations Mission in the Sudan (UNMIS)

REFERENCE: IAD: 09- 03183

FROM: Fatoumata Ndiaye, Acting Director
DE: Internal Audit Division, OIOS

SUBJECT: **Assignment No. AT2008/632/01 – Audit of information and communications technology**
OBJET: **governance and security management in UNMIS**

1. I am pleased to present the report on the above-mentioned audit.

2. 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 recommendations 13, 14 and 15. In OIOS' opinion however, these recommendations seek to address significant risk areas. We are therefore reiterating them 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 8, 11, 13, and 16), in its annual report to the General Assembly and semi-annual report to the Secretary-General.

cc: Mr. Farid Zarid, Chief of Staff, UNMIS
Mr. Nicolas von Ruben, Acting Director of Mission Support, UNMIS
Mr. James Boynton, Chief Integrated Support Services, UNMIS
Mr. Denfern Simpson, OIC CITS, UNMIS
Mr. Tom Sawyer, Chief IT, UNMIS
Mr. Swatantra Goolsarran, Executive Secretary, UN Board of Auditors
Ms. Susanne Frueh, Executive Secretary, Joint Inspection Unit
Mr. Moses Bamuwamye, Chief, Oversight Support Unit, Department of Management
Mr. Byung-Kun Min, Special Assistant to the USG, OIOS
Ms. Eleanor T. Burns, Chief, Peacekeeping 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

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

CHIEF, PEACEKEEPING AUDIT SERVICE:
Eleanor T. Burns: Tel: +1.917.367.2797, Fax: +1.212.963.3388,
e-mail: burnse@un.org

EXECUTIVE SUMMARY

Audit of information and communications technology governance and security management in UNMIS

OIOS conducted an audit of information and communications technology (ICT) governance and security management in the United Nations Mission in the Sudan (UNMIS). The overall objective of the audit was to assess the adequacy and effectiveness of ICT governance and security management within UNMIS. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

The results of the audit indicated the presence of unmitigated risks in the governance of ICT resources and the security of ICT operations. While UNMIS already took significant steps toward the strengthening of its ICT controls, there are still several areas that require adequate attention by Management. These areas include:

(a) The absence of a local ICT Review Committee;

(b) Lack of staff with adequate ICT expertise;

(c) Work plans not standardized and not available for all units;

(d) No mission-specific ICT risk assessment and security documentation;

(e) Policies and standard operating procedures not documented;

(f) Inadequate performance of communication links between Khartoum and the team sites;

(g) A high rate of hardware failures;

(h) Lack of standard project management methodology;

(i) Undocumented ICT security standards;

(j) No vulnerability assessments performed;

(k) Inadequate network security;

(l) Insecure transmission of data sent through digital senders; and

(m) Business continuity and disaster recovery for ICT operations still in draft form.

TABLE OF CONTENTS

Chapter		Paragraphs
I.	INTRODUCTION	1 - 4
II.	AUDIT OBJECTIVES	5 – 6
III.	AUDIT SCOPE AND METHODOLOGY	7
IV.	AUDIT FINDINGS AND RECOMMENDATIONS	
	A. Organization and governance	8 - 11
	B. Planning	12 - 18
	C. Policies and standards operating procedures	19 - 26
	D. ICT assets	27 - 30
	E. Project management	31 – 35
	F. ICT security management	36 – 73
	G. Status of previous audit recommendations	74 – 75
V.	ACKNOWLEDGEMENT	76
	ANNEX 1 – Status of Audit Recommendations	

I. INTRODUCTION

1. The Office of Internal Oversight Services (OIOS) conducted an audit of information and communications technology (ICT) governance and security management in the United Nations Mission in the Sudan (UNMIS). The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

2. The UNMIS Communications and Information Technology Service (CITS) is mandated to deliver voice, video and data services and support the information and communications network and applications for all Mission locations. The results of the ICT activities reported in the "Performance report on the budget of the United Nations Mission in the Sudan for the period from 1 July 2006 to 30 June 2007", A/62/749, indicated that CITS ensured support and maintenance for:

(a) 237 servers;
(b) 3,162 desktops;
(c) 955 laptops;
(d) 850 printers;
(e) 191 scanners; and
(f) 40 locations within the Mission area.

3. In terms of financial resources, the same document reported the following operational costs for information technology and communications for fiscal year 2006-2007:

Operational Costs	Apportionment (in $'000)	Expenditure (in $'000)
Communications	37,128.3	37,276.1
Information technology	17,284.1	21,820.6
Total	54,412.4	59,096.7

4. Comments made by UNMIS are shown in *italics*.

II. AUDIT OBJECTIVES

5. The main objectives of the audit were to determine whether controls in the areas of ICT governance and security were adequate. In particular, the audit assessed whether:

(a) An organizational structure was in place to govern, manage, and protect ICT resources and data;
(b) Processes existed for ICT strategic planning, monitoring, reporting, and continuous improvement;
(c) Adequate mechanisms were in place to identify and manage ICT risks;
(d) Mission specific ICT policies, and standard operating procedures were in place;
(e) ICT assets were adequately managed;

(f) ICT projects and initiatives were based on defined and standard management methodologies; and

(g) ICT security was managed on the basis of defined policies and procedures, including risk assessments and systematic vulnerability testing.

6. In addition, the audit included a review of the status of previously issued recommendations in the area of ICT management.

III. AUDIT SCOPE AND METHODOLOGY

7. Interviews were held with representatives from CITS, support and substantive offices in Khartoum and Juba. Documentation, including responses to audit questionnaires, was obtained and reviewed to ascertain the ICT governance structure and security environment. Tests, including network vulnerability tests, were undertaken to confirm the adequacy of controls and to identify threats, risks and vulnerabilities that may affect the ICT control environment.

IV. AUDIT FINDINGS AND RECOMMENDATIONS

A. Organization and governance

Lack of staff with adequate ICT security expertise

8. A competent workforce should be maintained for the creation and delivery of ICT services to the Mission's operations. This process is critical, as the recruitment and retention of skilled staff are important assets, and the governance of an effective internal control environment is heavily dependent on the motivation and competence of personnel.

9. Although UNMIS has recently completed the recruitment for ten vacancies in CITS, OIOS found the following weaknesses in the area of ICT human resources management:

(a) Lack of a dedicated resource for ICT security;

(b) Lack of subject-matter expertise on standard technologies that are implemented across missions (i.e., CCTV systems for physical security, and fire alarms systems for computer rooms); and

(c) Recruitment challenges and limitations of the current procedures, such as:

- The issuance of vacancy announcements based on a generic job profile to fill positions that are instead based on specific ICT skills (i.e. the two ICT pools of expertise for network and server groups); and
- Vacancy announcements that do not indicate the duty station, often leading to eligible candidates not accepting the position at an advanced stage in the recruitment process.

10. Inadequate staffing of the ICT function presents risks associated with the potential inability of the Mission to support critical functions, increase in the number of incidents or errors and dissatisfaction of staff members.

Recommendation 1

(1) The UNMIS Division of Mission Support should coordinate with the Department of Field Support to address the specific needs of the ICT function for the recruitment of staff specializing in ICT security-related disciplines.

11. *The UNMIS Division of Mission Support accepted recommendation 1 and stated that it will continue to coordinate with DFS to address the recruitment of specialized staff.* Recommendation 1 remains open pending submission to OIOS of documentation showing the actions taken to recruit staff specializing in ICT security-related disciplines.

B. Planning

Work plans not standardized and not available for all units

12. A work plan is required to manage and direct all ICT resources in line with the Mission's strategy and priorities. The work plan would improve key stakeholders' understanding of ICT opportunities and limitations, specify objectives, assess current performance, identify local capacity and human resource requirements, and clarify the level of investment required.

13. UNMIS has defined its ICT objectives and planned results in the "Budget for the United Nations Mission in the Sudan for the period from 1 July 2008 to 30 June 2009" (A/62/785), as follows:

(a) Disaster recovery and business continuity;
(b) Videoconference network services; and
(c) ICT development.

14. In addition, OIOS was provided with a draft of the "vision paper" for the period 1 July 2009 to 30 June 2010, developed by the Information and Communications Technology Division (ICTD) at New York Headquarters. This document defined the strategic direction for ICT operations with regard to: (a) the Wide Area Network; (b) mission support; (c) resource management; (d) ICT governance; (e) enterprise systems; (f) ICT security; and (g) operating systems.

15. While the annual budget of UNMIS defined at a macro level the main ICT objectives of the Mission, the corresponding work plans for their implementation have not been consistently developed. OIOS obtained the work plans only for a limited number of units, such as: (a) the Application Support Unit; (b) the Network Management Unit; (c) the Server Management Unit; and (d) the User Support Unit. However, these work plans were not standardized to

promote a common way of working. No work plans were available for the remaining units, composed of:

(a) Satellite communications;
(b) Private Automatic Branch Exchange (PABX);
(c) Special equipment;
(d) Microwave communications;
(e) VHF/HF communications;
(f) Rigging & Safety;
(g) Infrastructure/Service installations;
(h) Telephone billings;
(i) UNMIS switch board;
(j) Communications center; and
(k) Regional support.

16. OIOS acknowledged the important initiative taken by DFS/ICTD with the issuance of the "vision paper" for 2009-2010, contributing to the definition of a clear strategic direction for ICT operations at the mission level. However, this process must be complemented by Mission-specific work plan to translate the strategic goals and priorities established at Headquarters into the Mission specific plans of actions. In the absence of clearly defined work plans for all the units involved in carrying-out the ICT operations at the Mission level, UNMIS is exposed to the risks of allocating and using resources for activities not aligned with the strategic goals of the Organization, not focusing on the right priorities, and being unable to identify and leverage opportunities for improvements.

Recommendations 2 and 3

The UNMIS Division of Mission Support should:

(2) Ensure that all units in the Communications and Information Technology Section develop and communicate a work plan based on a standardized structure; and

(3) Develop and implement procedures to systematically monitor the implementation of ICT work plans. This process should include defining relevant performance indicators, a schedule for the timely reporting of performance, and prompt action upon deviations.

17. *The UNMIS Division of Mission Support accepted recommendation 2 and stated that unit work plans are primarily internal working documents that CITS uses to organize and monitor the various projects that it undertakes. As the work plans are unit specific, there is no perceived need that they be similar in appearance or standardized. Furthermore, the work plans contain a high content of technical jargon that is largely targeted to specific audience engaged in executing the plan, i.e., CITS. CITS will, however, review the work plan formats to see if there are any standardization opportunities, although this should not be limited to CITS.* Recommendation 2 remains open pending submission to OIOS

of documentation showing that standard work plans have been developed and communicated to all staff in CITS.

18. *The UNMIS Division of Mission Support accepted recommendation 3 and stated that CITS' participation in various Mission projects directed at the implementation of the Mission mandate are already incorporated within Mission project plans along with all the other participating/contributing specialist sections. Monitoring is and always has been in terms of deliverables according to the time frames built into the Mission deployment plans. CITS is but one of several enabling sections and CITS' contribution is not managed in isolation of the other interdependent project contributors. The Division of Mission Support, however, acknowledges that there is always scope for improvement and will examine opportunities for enhancing monitoring and reporting mechanisms.* Recommendation 3 remains open pending submission to OIOS of documentation showing the establishment of procedures to systematically monitor the implementation of ICT work plans, with defined performance indicators, a reporting schedule and a process to promptly act on deviations.

C. Policies and standard operating procedures

Policies and SOPs not formally approved

19. To ensure the proper use, support and continuity of operations, it is necessary to provide technical staff and end-users with documented policies and SOPs for applications and infrastructure.

20. CITS drafted policies and SOPs for the following activities:

(a) Communication centre;
(b) Server management;
(c) Communications, information technology and information systems for field mission, and their interaction with CITS at Headquarters (draft);
(d) Mercury support; and
(e) UNMIS electronic mail policy and guidelines.

21. In addition, CITS also referenced the operating procedures for incident management, issued by the United Nations International Computing Centre, Support Team at Brindisi, and the policy directives issued, in draft form, by ICTD. These directives specified the requirements for for ICT security business continuity and emergency preparedness.

22. Since most of the policies and standard operating procedures developed or referenced by CITS are still in draft form, there is a risk that staff would not comply with ICT policies and standards, and UNMIS will not be able to ensure effective monitoring, oversight, and enforcement of the established requirements.

Recommendation 4

(4) The UNMIS Division of Mission Support should review, update and formalize all policies, standard operating procedures and guidelines related to ICT operations.

23. *The UNMIS Division of Mission Support accepted recommendation 4 and stated that Headquarters has been working for some time to issue a comprehensive range of standardized CITS SOPs that would be implemented by all missions. The purpose of this initiative is to ensure some degree of common approach and remove the wasteful duplication of effort in missions where every mission is independently developing virtually identical documents. The issuance of those standardized SOPs is taking place progressively and usually takes the form of a draft (for mission input) in the first iteration. Where UNMIS CITS has internal SOPs, these are simply interim solutions pending finalization of the standardized SOPs. As the various standardized SOPs are finalized and released, UNMIS CITS will adopt them, subject to review and modification to accommodate the Mission's unique needs. The SOPs will then be submitted for endorsement by UNMIS Management. This will be an ongoing process.* Recommendation 4 remains open pending submission to OIOS of copies of finalized policies, standard operating procedures and guidelines related to ICT operations.

Inadequate bandwidth of communication links between Khartoum and team sites

24. Effective data management practices require the identification of information needs and the monitoring of infrastructure performance to help ensure the quality, timeliness and availability of organizational data.

25. The results of the interviews conducted with the staff of UNMIS, indicated that the bandwidth of the communication links between UNMIS Khartoum Office and team sites (128 Kb per second), was considered to be inadequate. This inadequacy was addressed by the expression of interest issued by UNMIS for the provision of internet satellite bandwidth to upgrade services of 20 UNMIS team sites (contracted in February 2009; UNMIS/CON/09/15). In this regard, OIOS noted the need for constant monitoring of the data requirements and performance of the team sites, considering also that all voice communications links within the Mission's sites rely on the connection with Khartoum, thus representing a single point of failure.

Recommendation 5

(5) The UNMIS Division of Mission Support should assess the data requirements and data performance needs of the team sites and reassess network load together with the bandwidth between the Khartoum Office and team sites.

26. *The UNMIS Division of Mission Support accepted recommendation 5 and stated that this is an ongoing process and that continuous assessments are being made to provide optimum performance. OIOS was informed that the*