INTERNAL AUDIT DIVISION

OFFICE OF INTERNAL OVERSIGHT SERVICES

AUDIT REPORT

Management of information and communication technology at UNMIS

25 October 2007
Assignment No. AP2006/632/06

United Nations Nations Unies

INTEROFFICE MEMORANDUM MEMORANDUM INTERIEUR

INTERNAL AUDIT DIVISION · DIVISION DE L'AUDIT INTERNE
OIOS · BSCI

TO: Mr. Taye Zerihoun
A: Acting Special Representative of the Secretary-General
United Nations Mission in the Sudan

DATE: 25 October 2007

REFERENCE: AUD-7-5:26 (07- 00671)

for

FROM: Dagfinn Knutsen, Director
DE: Internal Audit Division, OIOS

SUBJECT: **Assignment No. AP2006/632/03: Management of information and**
OBJET: **communication technology at UNMIS**

1. I am pleased to present the report on the above-mentioned audit, which was conducted during October 2006 to February 2007.

2. Based on your comments, we are pleased to inform you that we will close recommendations 12 and 13 in the OIOS recommendations database as indicated in Annex 1. In order for us to close the remaining 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. Please note that OIOS will report on the progress made to implement its recommendations, particularly those designated as critical (i.e., recommendations 1, 4, 6, 7 and 8), in its annual report to the General Assembly and semi-annual report to the Secretary-General.

4. IAD is assessing the overall quality of its audit process and kindly requests that you consult with your managers who dealt directly with the auditors and complete the attached client satisfaction survey form.

cc: Mr. Kiplin Perkins, DOA, UNMIS
Mr. Philip Cooper, Director, DFS
Mr. Swatantra Goolsarran, Executive Secretary, UN Board of Auditors
Mr. Jonathan Childerley, Chief, Oversight Support Unit, Department of Management
Mr. Byung-Kun Min, Programme Officer, 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

ACTING CHIEF, PEACEKEEPING AUDIT SERVICE:
William Petersen: Tel: +1.212.963.3705, Fax: +1.212.963.3388,
e-mail: petersenw@un.org

EXECUTIVE SUMMARY

Management of information and communication technology at UNMIS

OIOS conducted an audit of the management of information and communication technology in UNMIS from October 2006 to February 2007. The main objectives of the audit were to determine whether: (i) ICT assets were managed, maintained and disposed of appropriately; (ii) a communication and IT security management structure was in place; and (iii) telephone billing was managed in line with applicable rules. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

The Mission had an inventory of 26,724 non-expendable ICT assets, valued at almost $46 million and 58,817 expendable items valued at almost $5 million as at 31 October 2006. The inventory controls were inadequate to manage and maintain such a large inventory. Although the current record of receipt and issue of assets for the Mission HQs was complete, data entry for certain locations was incomplete. There was also a backlog of data entry relating to manual vouchers for 2005. All receipt and issue vouchers were not readily traceable.

Inaccurate record-keeping and non-completion of physical verifications by the Communication and Information Technology Section (CITS) and Property Control and Inventory Unit (PCIU) generated a category of "unaccounted for" assets. Management did not have precise knowledge of the location of these assets, which were being used although the issue vouchers for such assets were missing or stolen. CITS estimated that there were 1,904 such assets valued at $4.1 million as at 13 February 2007. CITS and PCIU attributed the number of unaccounted assets to the shortage of staff.

CITS has implemented ICT security measures with the adoption of an antivirus programme (Symantec) and firewalls. It also filters e-mail attachments to prevent attacks by viruses and hackers. The Section was keeping a backup of all the Lotus Notes and shared drives to comply with the DPKO policy on disaster recovery. However, CITS lagged behind in framing CITS information security policy after conducting risk assessment exercise and adopting internal controls. The Mission management has not developed and tested any disaster recovery and business continuity plans for information security or established backup centers away from headquarters. The Mission also needs an automated intrusion detection system to strengthen the monitoring mechanism against unauthorized intrusion into the systems.

The telephone billing system was working satisfactorily. However, the recovery rates for personal calls from the staff were higher than the charges applied by the operator because the predetermined call rates being applied by the Mission did not match the rates of the vendor. This led to excessive recovery of approximately 229,207 Euros in phone charges from the staff as compared to the bills received from the service provider from June 2005 to October 2006. There is therefore a need to review the call rates being charged to the staff for personal calls.

OIOS made a number of recommendations to address the above weaknesses. UNMIS accepted all the recommendations and has initiated action to implement them.

TABLE OF CONTENTS

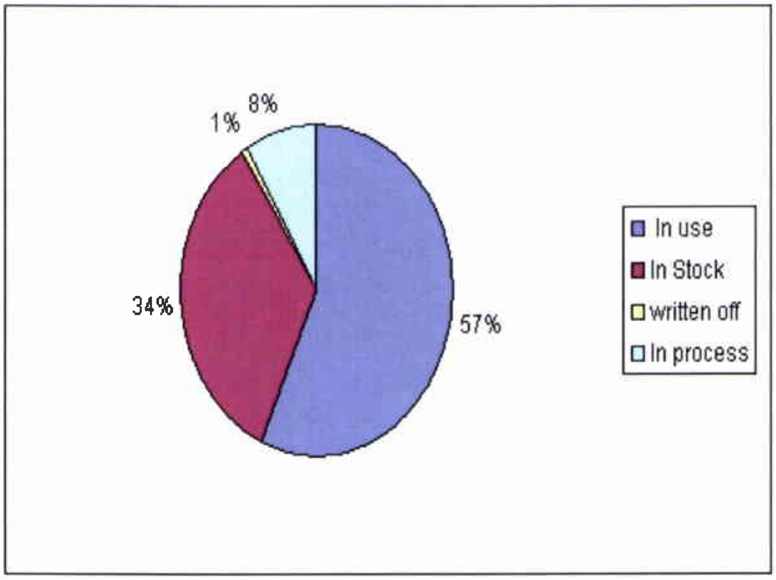
I. INTRODUCTION

1. OIOS conducted an audit of the management of information and communication technology (ICT) at UNMIS from October 2006 to February 2007.

2. The Mission's budget for communication and information technology was $54,421,000 in financial year 2004/05 and $58,966,000 in 2005/06. The Communications and IT Section (CITS) is responsible for providing communications and IT services including installation, operation and maintenance of communications infrastructure and systems.

3. CITS consists of four units: (a) the Communications Unit, responsible for telecommunication operations; (b) the Information Technology Unit (ITU), responsible for the operation of networks and information systems; (c) the Asset Management Unit (AMU), responsible for the management of non-expendable and expendable ICT assets; and (d) the Billing Unit, responsible for telephone bills. CITS had an authorized staffing of 79. As of 31 October 2006, it had 66 staff members.

Figure 1: CITS non-expendable assets as of 31 October 2006



4. CITS had an inventory of 26,724 non-expendable assets valued at $45,906,000 and 58,817 expendable items valued at $4,739,000 as at 31 October 2006. The Communications Unit was responsible for 63 per cent of the non-expendable inventories, and the IT Unit controlled 37 per cent of the inventories. The inventories consist of state of the art telecommunication and IT equipment, including satellite dishes, communication networks, wireless networks and computer servers. The Mission has warehouses at Khartoum and El-Obeid to store the inventory. The Khartoum warehouse provides storage services to four sections, namely, CITS, Engineering, Supply and Medical Services. The CIT assets in El-Obeid are stored in containers.

5. The information security programme is intended to protect the Mission's digital information and other critical information assets. Managing information security is primarily the responsibility of the Mission's top management, and involves *inter alia*, commitment to keeping risks associated with information systems under control, and allocating adequate resources for effective information security.

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

II. AUDIT OBJECTIVES

7. The objectives of the audit were to assess whether:

a) ICT assets are appropriately managed, maintained and disposed of;
b) An appropriate communication and IT security management structure is in place; and

c) Telephone billing is managed effectively to protect the Organization's interests.

III. AUDIT SCOPE AND METHODOLOGY

8. The audit reviewed the Mission's policies, strategies, and management processes for safeguarding its communication and information technology assets. OIOS examined asset management and inventory control procedures and reviewed telephone billing records to evaluate the billing process and to ensure the Mission's interests are protected. The audit also assessed the CITS management structure to determine if it is able to achieve the Mission's objectives.

9. The audit approach involved reviewing relevant documentation, observing the system, and analyzing internal controls. OIOS also interviewed the key CITS personnel involved in the operation and management of Mission information systems. The auditors also visited the data centers, server rooms and warehouses in Khartoum and Al-Obeid.

IV. AUDIT FINDINGS AND RECOMMENDATIONS

A. Asset management

State of records

10. Although the current record of asset receipts and issues for the Mission HQs was complete, the data for certain locations was incomplete. There was a backlog of data entry relating to manual vouchers for 2005. CITS used manual vouchers for issuing items to users in the sectors during 2005. Further, Regional

Administrative Officers (RAOs) did not punctually return the manually issued vouchers after obtaining the signatures of the person receiving the assets. As a result, a large number of vouchers was not entered in the system.

11. Not all receipt and issue vouchers were readily traceable as the records were stored in boxes. From a sample of 100 non-expendable assets, the AMU could only provide 11 issue vouchers and no receipt vouchers. Similarly, from a sample of 50 expendable items, it could not provide any issue or receipt vouchers. The AMU attributed these deficiencies to problems in the Galileo system.

12. In response to an audit query concerning the location of expendable assets records, the AMU conceded that they had not entered 80 per cent of expendable assets into Galileo by 31 October 2006. The AMU staff explained that the backlog in entering vouchers of expendable assets into Galileo was attributable to the fact that during the early period of the Mission, AMU issued assets using manual vouchers due to the shortage of Galileo-trained staff.

13. The PMM, paragraph 3.7 requires that after completion of receiving and inspection by R&I, the asset should be recorded in Galileo. OIOS tracked a sample of 20 reports to determine AMU's timeliness in updating Galileo. The time taken ranged between 1 and 34 days, which contributed to the backlog in updating the Galileo system.

14. CITS explained that the delays were caused mainly by a shortage of staff, compounded by the incorrect description of items inspected and data entry by the Receiving and Inspection (R&I) Unit, and the CITS requirement to test some sensitive items such as satellite phones before updating Galileo. However, when OIOS asked R&I staff about the reasons for the delays, they asserted that late inspections by CITS representatives were responsible. R&I staff noted that they immediately informed CITS by telephone when items arrive and sent formal written notice after three or four days. They claimed that CITS representatives usually arrive in four to five days after the initial call.

Accuracy of records

15. Inaccurate record-keeping and non-completion of physical verification by AMU and PCIU resulted in "unaccounted for" assets. Management did not have precise knowledge about these assets, which were either "under use" with missing issue vouchers, stolen or misplaced. CITS estimated the number of such assets as 1,904 (6.65 per cent) of its total inventory, and 11 per cent of the assets in use, but could not verify these estimates. OIOS estimated the value of these unaccounted for assets as $4.1 million as of February 13, 2007. CITS and PCIU attributed this state of affairs to the shortage of staff.

Evidence of issued assets

16. RAOs are responsible for managing United Nations Owned Equipment (UNOE) in sectors in accordance with Mission Administrative Instruction No. 02/2006. The RAOs issued assets in the sectors/team sites by using manual

vouchers, since they did not have access to Galileo. They are required to send the manual vouchers to CITS HQ for data entry. AMU explained that they did not have representation in the sectors. CITS technicians had an additional responsibility of distributing assets and obtaining issue vouchers from the users. However, the RAOs did not send such vouchers to CITS punctually. For example, of the 410 shipments to team sites, the concerned RAOs did not respond in 342 cases or 83 per cent, which hampers the updating of records. The response rate ranged from 60 per cent to 100 per cent. AMU explained that shortages of staff at headquarters and the lack of Unit staff at team sites made it difficult to maintain, update and monitor the inventory records.

Physical verification

17. Paragraph 5.30 of the Property Management Manual, requires that PCIU undertake physical verification of non-expendable assets at regular intervals, at least once a year. DPKO policy instructions, procedures and guidelines for control of UNOE instruct PCIU to verify 10 per cent of all Mission records each month. PCIU did not complete this physical verification, but verified 82 per cent of the Mission's total non-expendable assets during the period 1 July, 2005 to 31 December. 2006. However, the Unit could not provide a physical verification report.

18. CITS also could not undertake a physical verification at Khartoum and team sites and advised that they had verified 84 per cent of their assets during September-November 2006 at all the sectors. However, they also could not provide any physical verification reports.

19. In order to evaluate controls at the warehouses and check the accuracy of records, OIOS conducted a physical count of the CITS assets at the Khartoum warehouse on 10 December 2006. The results showed the following discrepancies:

- Out of a sample of 1,239 non-expendable assets reported to be in inventory, 707 items were not available in the warehouse; conversely, 51 items had not been recorded, even though they were physically available in the warehouse.

- Out of 2,928 expendable assets, 412 items were not recorded in Galileo, while 191 items were short in the warehouse.

20. According to management, the shortage of staff, improper priorities, and day to day work load caused the weaknesses in applying various inventory controls. There was no audit trail to ascertain the accurate status of inventory and determine number of unaccounted for assets. As a result, OIOS was not able to confirm the accuracy, completeness and reliability of inventory balances.

21. During the exit conference, the DOA advised that the Mission was aware of the problem and was establishing a separate Property Management Section. The section would be responsible for the entire cycle of inventory management. The system of dual responsibility for managing assets by the PCIU and Self-

accounting Units (SAUs) would be discontinued. The Mission administration also provided documentation concerning the plans to establish the new section. OIOS recognizes the Mission's initiative to address the problem.

Recommendations 1 and 2

The UNMIS Administration should:

(1) Ensure that, as soon as the Property Management Section is established, standard operating procedures relating to the receipt, issue and disposal of assets are issued and circulated among the Mission staff; and

(2) Establish a task force to clear the backlog of data entry for unrecorded assets and issues to users, and to reconcile the asset records.

22. *The UNMIS Administration accepted recommendation 1 and stated that the Property Management Section (PMS) has effectively taken over the asset management functions from CITS on 1 September 2007. PMS will combine all SAUs' standard operating procedures based on established asset management standards set by DPKO to form one PMS SOP*. Recommendation 1 remains open pending confirmation by the Mission that the SOPs have been approved and implemented.

23. *The UNMIS Administration accepted recommendation 2 and explained the various actions taken by the Mission, including the hiring of additional staff, to clear the backlog*. Recommendation 2 remains open pending confirmation by the Mission that the backlog has been cleared and the reconciliation of inventory records has been completed.

Warehouses

24. Generally accepted management principles require prudent and systematic management of warehouses with adequate manpower, proper facilities such as section partitioning, secured locks for each section, controlled temperature and adequate recordkeeping. CITS has two warehouses one each at Khartoum and El-Obeid, and it is sharing a warehouse at Khartoum with other sections – Supply Section, Engineering and Medical Service. There is also a common area for R&I. However, this warehouse does not have adequate space to accommodate the assets of the four sections.

25. The Mission was not managing warehouses at Khartoum and El-Obeid in an organized manner. The conditions at the warehouse in Khartoum were particularly serious. There were no partitioning walls for assets belonging to different sections. All staff of the four sections had unrestricted access to the entire warehouse. No one section was responsible for the safety and security of the stored items. The common area for the R&I Unit had no partitioning without any specific security arrangements. The assets remained in the custody of R&I without being recorded in Galileo until completion of the R & I process. The

storage of such assets in a common area was risky, as nobody could be held responsible for any loss. Many items were stolen in the past from R&I area before the items were received and inspected.

26. Proper shelves, cupboards or bins with adequate markings were not available in the warehouses. Most of the CITS assets were stored in boxes on a dusty floor. CITS was storing high value equipment in containers for security reasons. The walls of the warehouse and containers were not marked with bar codes shown in Galileo to identify the assets. Therefore, an inventory item shown in Galileo as stored in the warehouse might require searching all the boxes and containers containing CITS stores.

27. The temperature inside the warehouse was not controlled, although some items such as toners and electronic equipment were temperature-sensitive. The containers in the warehouse where high-value items were stored were dark and hot. The equipment which was stored for an extended period had become rusty.

28. Physical security of the warehouses was inadequate. The back gate could not be shut properly, and although thefts had taken place in the Khartoum warehouse, security measures had not been improved. International security personnel were not deployed to monitor warehouse security. There were not enough fire extinguishers and no emergency exits, although the assets and material were fire-prone. There was a door in the back of the warehouse, but many store items were piled in front of it, so it would be difficult to use it in case of an emergency. There was a separate room for written-off CITS assets awaiting disposal, but these were piled up on the floor in a disorganized manner. There was a risk that these might be stolen before disposal.

29. At the El-Obeid warehouse, CITS used 56 containers for storing equipment. Some items such as cables were located outside the containers. This warehouse had the same problems as those at the Khartoum warehouse. OIOS could not follow the inventory lists provided to trace the assets as the locations shown in the list were incorrect and some of the items sampled (e.g., batteries) were scattered in many different containers.

Recommendation 3

(3) The UNMIS Administration should review the conditions at the warehouses to ensure proper storage, security and recordkeeping, considering the temperature and space requirements for different categories of assets.

30. *The UNMIS Administration accepted recommendation 3 and stated that the Mission has closed the Khartoum warehouse and transferred CITS equipment as an interim arrangement in seven sea containers and seven refrigerated containers. The equipment will be stored in the new warehouses to be constructed at El Obeid.* Recommendation 3 remains open pending receipt of confirmation by the Mission of the transfer of CITS equipment from its current location to the new warehouses at El Obeid.

B. Information security policy and administration

31. CITS has implemented ICT security measures with the adoption of an antivirus programme (Symantec) and firewalls. CITS had been filtering e-mail attachments since November 2006 after a query by OIOS during audit field work. The section was backing up all Lotus Notes and shared drives to comply with the DPKO policy on disaster recovery.

Risk assessment exercise

32. The Secretary-General's report A/59/265, "Information Technology Strategy", fixed the target date for completion of the risk assessment exercise to estimate the risks to the information technology operations in the missions by the end of 2004. A risk assessment exercise should be undertaken to proactively identify, monitor and control the key risks to the missions. It should cover all vulnerable areas like CIT operations, assets protection, hardware and software management, applications, Lotus Notes and web-based services. The management may evaluate, by performing the risk assessment exercise, the criticality of its important CITS systems and equipment, and their vulnerability. OIOS found that CITS management had taken steps to safeguard the confidentiality, integrity and availability of Mission information, but had not carried out any formal risk assessment exercise. Hence, they did not comply with the instructions from UNHQ.

Recommendation 4

(4) The UNMIS Administration should, in compliance with Secretary-General's report A/59/265 on Information Technology Strategy, undertake a risk assessment exercise covering all areas of communication and information technology and evaluate relevant controls for mitigating risks.

33. *The UNMIS Administration accepted recommendation 4 and explained that the Mission is in the process of recruiting necessary staff to undertake the exercise*. Recommendation 4 remains open pending receipt of a copy of the risk assessment report from the Mission.

CITS security policy

34. CITS was complying with the DPKO policy of providing ICT services, as spelled out in LSD/OMS/DPKO memorandum no. 2006-UNHQ-065326 dated 16 May 2006. The policy circulated by DPKO was part of a series of several policy guidelines that formed a comprehensive framework. The DPKO policy provided a generalized guideline for all the missions, but Mission management had not carried out a risk assessment exercise and had not developed a Mission-specific information security policy.

Recommendation 5

(5) The UNMIS Administration should develop an information security policy after performing a comprehensive risk assessment exercise and circulate it widely to CITS staff and general users of CIT equipment and systems.

35. *The UNMIS Administration accepted recommendation 5 and indicated that the present IT security policy will be updated and reissued by 30 September 2007.* Recommendation 5 remains open pending receipt of a copy of the IT security policy.

Disaster recovery and business continuity (DRBC) plan

36. Disaster recovery and business continuity plans ensure protection of information and restoration of information processing systems in case of a major disaster or evacuation. CITS is following DPKO Policy Instructions No. 2006-UNHQ-024582 of 20 July 2004 and No. 2006-UNHQ-077816 dated 1 November 2006. CITS took some steps to implement these guidelines, but these efforts needed improvement as discussed below.

37. CITS had no Mission-specific DRBC policy document nor had it developed a plan for providing logistics support to CITS for handling a major disaster.

38. The Mission had not established the two types of backup centers: one off-site in Sudan and the other in another country as prescribed by the DPKO policy guidelines. CITS had selected El-Obeid as regional backup centre, but Mission management had not yet decided to hire space for servers, a data centre and a warehouse at that location. CITS had selected Entebbe (Uganda) as the neighboring country backup centre, but no progress had been made so far in actually setting up the centre.

39. CITS had developed a draft DRBC Standard Operating Procedure (SOP). However, the SOP did not consider the scenario of losing control of the infrastructure in Khartoum and the evacuation of employees. It did not specify the duties and procedures of respective staff and sections in such an eventuality.

40. The Mission never tested the DPKO DRBC plan or the CITS DRBC Standard operating procedure because CITS felt that such testing would interrupt critical Mission services. Also, such testing would require prior notification of DPKO, as it would interrupt the Mission's critical communication systems. In OIOS' view this explanation is not satisfactory as testing is essential because in case of a disaster, the loss of information could be critical. The Mission could utilize other methods of testing like structured walk throughs and phased testing without jeopardizing the vital communication systems with UNHQ and Brindisi log base.

41. CITS had not maintained stockpiles of essential CIT equipment outside Khartoum, which according to the Chief Communication and Information Technology Section (CCITS) was due to the lack of warehousing facilities.

42. The Mission had not taken steps to educate and train management and staff about DPKO's DRBC policy as required by DPKO. The staff member in-charge of payroll was not aware of any DRBC plan. The System Administrator in Finance noted that he had heard about the DRBC plan, but was not aware of its details or his responsibilities in an emergency situation.

Recommendations 6 to 8

The UNMIS Administration should:

(6) Develop and submit for approval by the Mission's management a comprehensive Mission-specific disaster recovery and business continuity plan, spelling out the procedures to respond to a disaster, strategy for data recovery and allocation of resources required to implement the plan;

(7) Prepare a plan to train CITS staff in business disaster and recovery planning through practical exercises and periodic testing of the plan; and

(8) Take expeditious action to establish backup centers at El-Obeid and at Entebbe to ensure that the Mission can quickly restore its normal operation in case of an emergency or disaster at the mission HQs in Khartoum.

43. *The UNMIS Administration accepted recommendation 6 and provided a draft of the Mission's DRBC Policy and Information Circular, which will be improved and finalized by June 2008. UNMIS further explained that CITS is maintaining a backup of systems in Khartoum and sector HQs on a daily, weekly and monthly basis. Mission critical data and mail are transferred regularly to UNLB for backup purposes.* Recommendation 6 remains open pending receipt of confirmation by the Mission that the DRBC plan has been fully implemented.

44. *The UNMIS Administration accepted recommendation 7 and indicated that CITS is drafting a request for proposal to hire trainers. The Mission is also arranging a "training of trainers" for its staff.* Recommendation 7 remains open pending receipt of documentation from UNMIS showing that CITS staff has been trained in disaster recovery and planning.

45. *The UNMIS Administration accepted recommendation 8 and stated that the Mission plans to have an offsite mobile backup at Khartoum Airport and at El-Obeid. It further clarified that instead of Entebbe, Brindisi and Valencia have been identified as offsite DRBC locations.* Recommendation 8 remains open pending confirmation by the Mission of the establishment and functioning of offsite backup centers.

Network security

46. Network security is necessary to keep the Mission systems secure against unauthorized access, manipulation, and use by outsiders. Organizations can secure their networks by limiting the services that are available and installing devices that deny unauthorized requests for access to services and data. OIOS found that CITS was using firewalls and Cisco switches for monitoring network operations and defending against potential hackers' attacks. However, effective monitoring requires automated controls which give warnings concerning a virus or a hacker's attack. CITS required an Intrusion Detection System for enhancing the efficiency of the monitoring equipment. CITS advised that it was in the process of acquiring such a system.

Recommendation 9

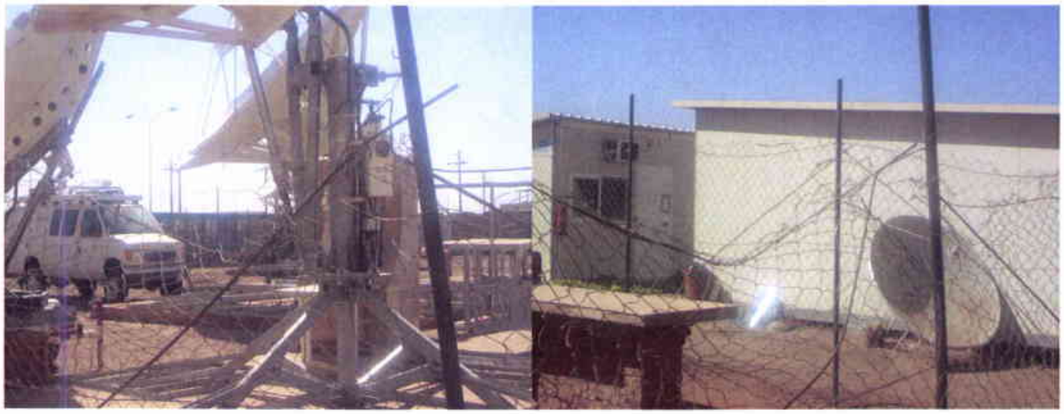
(9) The UNMIS Administration should acquire and install an automatic intrusion detection system as soon as possible to ensure effective protection of networks against malicious attacks.

47. *The UNMIS Administration accepted recommendation 9 and indicated that an intrusion detection system will be procured shortly.* Recommendation 9 remains open pending confirmation by the Mission of the procurement and installation of an intrusion detection system.

Information security controls

48. CITS staff was aware of the importance of protecting the Mission's information system. However, there was a need for the following improvements:

Examples of broken fences



a) The main communication installations were located behind the server rooms near the south entrance of the H/Qs building. This area, had been cordoned off with wire fencing, but the area was accessible from a number of places. The wire had become weak in two places. After the exit conference, the Engineering Section started the work of repairing and mending the fence wires.

b) There was no closed-circuit TV (CCTV) system in the server rooms and CITS installations. CITS advised that based on OIOS' observation, it had requisitioned IP cameras for the server rooms.

c) The cabinets in the library used to store important papers, CDs and removable storage media devices, etc., were not fire-proof and did not have locks.

Recommendations 10 and 11

The UNMIS Administration should:

(10) Follow up with the Procurement Section with regard to obtaining and installing closed-circuit TV cameras to ensure proper surveillance in CITS installations and server rooms; and

(11) Ensure that safes are provided for storing removable storage media and master CDs.

49. *The UNMIS Administration accepted recommendation 10 and stated that it has procured the cameras, which will be installed by 30 September 2007.* Recommendation 10 remains open pending confirmation by the Mission that the cameras have been installed.

50. *The UNMIS Administration accepted recommendation 11 and indicated that safes will be installed shortly and all removable media and master CDs will be stored in there.* Recommendation 11 remains open pending confirmation by the Mission of the installation of safes for the storage of removable storage media and master CDs.

Information security monitoring

51. Monitoring of security operations by senior management creates awareness of security issues among the staff and is also helpful in creating discipline. Effective monitoring results by generating periodic reports, scheduling regular meetings chaired by senior management, preparing information security action plans and incorporating information security as part of the Mission's overall security plan. OIOS could not identify any specific periodic reports relating to information security submitted by CITS to Mission senior management. Further, CITS could not provide any minutes of meetings on information security chaired by top management.

52. CITS managers advised that they submitted a weekly report to the Director of Administration (DOA) at the Mission headquarters and to Regional Administrative Officers (RAOs) in the sectors and team sites. These reports

contained information about jobs performed by the section in Khartoum and at team sites during the week. However, there was no specific report on information security issues. Similarly, no reports about information security were provided to the owners of the application systems, and the Mission had not developed any action plans for information security.

Recommendations 12 and 13

The UNMIS Administration should:

(12) Institute a mechanism of periodic reporting to senior management relating to information security; and

(13) Hold periodic meetings, chaired by the DOA or his nominee on information security to assist in monitoring information security policy and plans.

53. *The UNMIS Administration accepted recommendation 12 and indicated that it has been implemented. A monthly report is submitted to DOA that includes CITS specific information.* Based on the action taken by the Mission, recommendation 12 has been closed.

54. *The UNMIS Administration accepted recommendation 13 and stated that the DOA has nominated the Chief, ISS to assist in monitoring security policy and plans in a weekly meeting. Further, CISS keeps regular contacts with CITS to discuss and monitor information security issues.* Based on the action taken by the Mission, recommendation 13 has been closed.

Information security training and awareness programme

55. Information security awareness and training ensure that personnel at all levels understand their information security responsibilities. The DPKO ICT governance structure for field missions spelled out in 2005-UNHQ-047303 dated 3 August 2005 stressed the provision of adequate training and support as a precondition for cost-effective implementation of systems. However, the Mission did not have a training programme on information security. CITS also did not arrange for training the trainers who could then train the staff. CITS management advised that DPKO had planned a train the trainers programme in Brindisi in 2007. However, analysis of CITS staff job descriptions showed that their busy schedules did not allow time for training activities, and they did not have time to train the staff.

Recommendation 14

(14) The UNMIS Administration should provide information security training to CITS staff and general users of CIT equipment and systems.

56. *The UNMIS Administration accepted recommendation 14 and stated that the Mission is taking the same steps as described in its response to*

recommendation 7. Recommendation 14 remains open pending confirmation by the Mission that training on information security has been conducted.

C. ICT governance, organization and planning

57. ICT governance is the responsibility of the Mission senior management. It is an integral part of Mission management and consists of leadership, planning and organizational structures. ICT governance provides processes that ensure that the Mission's ICT activity sustains and extends the UNMIS mandate, strategy and objectives. OIOS found that mission management did not pay attention to the following governance issues:

ICT Review Committee

58. DPKO, in its circular OMS/DPKO dated 3 August 2005, required the establishment of ICT Review Committees (ICTRCs) at missions to be chaired by DOA/COA or his/her designated representative. The ICTRCs are intended to ensure inter alia, that the information and communication technology needs of Missions are properly identified and that mission information and communication technology projects and initiatives are aligned with the overall goals and priorities of the Department. However, Mission management did not establish an ICTRC. During the period from September 2005 to Oct 2006, CITS purchased equipment and software worth $916,310 with LCC approval and procured 43 items locally for $136,685. According to DPKO instructions quoted above, Mission management should have submitted these cases to ICTRC for approval.

Recommendation 15

(15) The UNMIS Administration should establish an Information & Communication Technology Review Committee as required by the Department of Peacekeeping Operations and ensure that all future ICT asset procurements are reviewed by the Committee.

59. *The UNMIS Administration accepted recommendation 15 and stated that it will be implemented in December 2008.* Recommendation 15 remains open pending confirmation by the Mission of the establishment of the ICT Review Committee.

Vacancy rate in CITS

60. CITS had an authorized international staffing level of 79 on 31 October 2006, but its actual strength was 66 resulting in a 16 per cent vacancy rate. It had 48 national staff members working against 175 authorized posts, resulting in a 73 per cent vacancy rate. CITS could not perform the following tasks until December 2006 due to the shortage of staff:

(a) Developing a Mission-specific information security policy;

(b) Developing and testing a Disaster Recovery and Business Continuity plan;

(c) Implementing a secure and reliable asset management programme and reliable warehousing operations; and

(d) Designing and implementing a training programme for CITS staff and general users

61. Although day to day operational work is being handled by junior staff, CITS has an acute shortage of professional staff to deal with policy matters and decision-making. The Chief Communication and Information Technology Section (CCITS), Chief Communication Officer (CCO) and Chief Information Technology Officer (CITO) are the only professionals who perform all of the specialized tasks relating to operational management, monitoring and reporting in the section. The CCO and CITO do not have professional deputies to help in executing work or assume responsibility in the absence of CCO or CITO. The field staff is not responsible for planning and operational management. The recent transfer of the CITO to another Mission may aggravate the problem.

Recommendation 16 to 18

The UNMIS Administration should:

(16) Take steps to fill the vacancies in the CITS on an urgent basis to ensure that key activities are carried out;

(17) Review the staffing table in the budget for 2007-08 for CITS to create a better balance between the professional and non-professional staff and to effectively perform necessary functions that are not being performed at present due to the shortage of staff; and

(18) Create an information security unit by internal reorganization and appoint an information security officer.

62. *The UNMIS Administration accepted recommendation 16 and stated that the process of hiring staff has been started.* Recommendation 16 remains open pending confirmation by the Mission that all vacant CITS posts have been filled.

63. *The UNMIS Administration accepted recommendation 17 and stated that additional staff requirements will be included in the budget proposal for fiscal year 2008-09.* Recommendation 17 remains open pending confirmation by the Mission that the CITS staffing table has been reviewed and adjusted.

64. *The UNMIS Administration accepted recommendation 18 and stated that the creation of an information security unit will be included in the budget proposal for fiscal year 2008-09.* OIOS acknowledges the Mission's response but wishes to reiterate that, in the interim, an information security unit should be

established by reorganizing the current structure to ensure that information security issues are given adequate attention.

D. Telephone billing

65. OIOS found that the Telephone Billing Unit (TBU) was generating, distributing and recovering telephone bills for personal calls on a timely basis.

Telephone bills for personal calls at excessive rates

66. The Mission has allowed its staff to make personal phone calls over the Mission system by using a personal identification number (PIN) code. The Mission recovers the personal phone call charges based on rates predetermined by UNHQ. Use of these predetermined call rates led to excessive recoveries of phone charges from the staff as compared to the bills received from the service provider. A comparison of the call rates billed by the operator and the predetermined rates being charged by the Mission disclosed an excess recovery of approximately 229,207 Euros from staff during the period June 2005 to October 2006. Details are shown in Annex 2.

Recommendation 19

(19) The UNMIS Administration should request DPKO to review the existing predetermined rates used to calculate recoveries from staff for private calls in UNMIS to bring the rates in line with the rates charged by the service provider, and consider the possibility of reimbursing the staff for overcharges.

67. *The UNMIS Administration accepted recommendation 19 and stated that it has implemented new call rates on 1 April 2007 after the approval of DPKO. However, the Mission indicated that it is unable to arrange the reimbursement of overcharges to staff because it involves international settlement between the UNMIS telecom operator and various other international telecom companies.* OIOS acknowledges the Mission's efforts to implement new call rates as well as the difficulties involved in reimbursing staff for the amounts overcharged. However, OIOS suggests that the Mission consult with the Controller on how to deal with the overcharges. Recommendation 19 therefore remains open pending receipt of documentation showing that the Mission was seeking to address the overcharges described above.

Outstanding mobile phone bills

68. TBU also recovers the costs of personal calls from mobile phones according to the prescribed rates. The Moabite bills amounting to 12,645,000 Sudanese Dinars recoverable from UNMIS staff were outstanding at October 2006. This situation arose primarily from a verbal instruction by a former Chief Administrative Officer (CAO) who stated that no recoveries should be made from staff if the bill was not submitted by the staff member to TBU.

Subsequently, TBU started recovering for 2005 bills. The recovery for outstanding bills for 2006 started in October 2006.

Recommendation 20

(20) The UNMIS Administration should take measures to recover the outstanding amounts (12,645,000 Sudanese Dinars) for personal calls on mobile phones.

69. *The UNMIS Administration accepted recommendation 20 and stated that it has recovered outstanding charges of SDD8, 453,634.45 to date and that the balance will be recovered shortly.* Recommendation 20 remains open pending confirmation by the Mission of the recovery of the remaining balance of personal mobile call charges.

V. ACKNOWLEDGEMENT

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

ANNEX 1

STATUS OF AUDIT RECOMMENDATIONS

Recom. no.	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
1	O	Confirmation by the Mission that the SOPs have been approved and implemented	31 December .2007
2	O	Confirmation by the Mission that the backlog has been cleared and the reconciliation of inventory records has been completed	31 December .2007
3	O	Confirmation by the Mission of the transfer of CITS equipment from its current location to the new warehouses at El Obeid	April 2008
4	O	Submission to OIOS of a copy of the risk assessment report	June 2008
5	O	Submission to OIOS of a copy of the IT security policy	30 Sep 2007
6	O	Confirmation by the Mission that the DRBC plan has been fully implemented	June 2008
7	O	Submission to OIOS of documentation showing that CITS staff has been trained in disaster recovery and planning	June 2008
8	O	Confirmation by the Mission of the establishment and functioning of offsite backup centers	December 2007
9	O	Confirmation by the Mission of the procurement and installation of an intrusion detection system	December 2007
10	O	Confirmation by the Mission that the cameras have been installed	30 Sep 2007
11	O	Confirmation by the Mission of the installation of safes for the storage of removable storage media and master CDs	30 Sep 2007
12	C	Action completed	Implemented
13	C	Action completed	Implemented
14	O	Confirmation by the Mission that training on information security has been conducted	June 2008
15	O	Confirmation by the Mission of the establishment of the ICT Review Committee	December 2008
16	O	Confirmation by the Mission that all vacant CITS posts have been filled	On going
17	O	Confirmation by the Mission that the CITS staffing table has been reviewed and adjusted	June 2008
18	O	Confirmation by the Mission of an interim information security unit	June 2008
19	O	Consultation by the Mission with the Controller on how to deal with the telephone overcharges	1 April 2007
20	O	Confirmation by the Mission of the recovery of the remaining balance of personal mobile call charges	30 Sep 2007

[1] C = closed, O = open

[2] Date provided by UNMIS in response to recommendations

ANNEX 2

Excess Recovery of Personal Telephone Charges

(1) Period	Amount (Euro)			
	(2) Service provider's total charges[1]	(3) Estimated personal calls (98%*Col 2)	(4) UNMIS recovery for personal calls	(5) Excess of personal call recoveries over total bill (Col 4-3)
Jul & Aug 2005	62,266.62	61,021.29	71,798.24	10,776.95
Sep & Oct 2005	76,845.09	75,308.19	87,171.16	11,862.97
Nov & Dec 2005	91,997.23	90,157.29	121,689.44	31,532.15
Jan & Feb 2006	122,020.10	119,579.70	154,993.57	35,413.87
Mar & Apr 2006	190,542.72	186,731.90	206,685.18	19,953.28
May & Jun 2006	222,109.63	217,667.40	248,530.60	30,863.20
Jul & Aug 2006	262,927.25	257,668.70	303,813.64	46,144.94
Sep & Oct 2006	302,595.27	296,543.40	339,202.93	42,659.53
TOTALS	1,331,303.91	1,304,677.87	1,533,884.76	229,206.90

UNITED NATIONS

OIOS Client Satisfaction Survey

Audit of: Management of ICT at UNMIS (AP2006/632/06)

	1	2	3	4	5
By checking the appropriate box, please rate:	Very Poor	Poor	Satisfactory	Good	Excellent
1. The extent to which the audit addressed your concerns as a manager.	□	□	□	□	□
2. The audit staff's understanding of your operations and objectives.	□	□	□	□	□
3. Professionalism of the audit staff (demeanour, communication and responsiveness).	□	□	□	□	□
4. The quality of the Audit Report in terms of:					
• Accuracy and validity of findings and conclusions;	□	□	□	□	□
• Clarity and conciseness;	□	□	□	□	□
• Balance and objectivity;	□	□	□	□	□
• Timeliness.	□	□	□	□	□
5. The extent to which the audit recommendations were appropriate and helpful.	□	□	□	□	□
6. The extent to which the auditors considered your comments.	□	□	□	□	□
Your overall satisfaction with the conduct of the audit and its results.	□	□	□	□	□

Please add any further comments you may have on the audit process to let us know what we are doing well and what can be improved.

Name:______________________ Title:______________________ Date:__________

Thank you for taking the time to fill out this survey. Please send the completed survey as soon as possible to:
Director, Internal Audit Division, OIOS
By mail: Room DC2-518, 2 UN Plaza, New York, NY 10017 USA
By fax : (212) 963-3388
By E-mail: knutsen2@un.org