



OIOS

Office of Internal Oversight Services

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

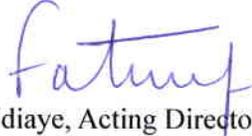
MEMORANDUM INTERIEUR

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

TO: Mr. Ashraf Jehangir Qazi,
A Special Representative of the Secretary-General
United Nations Mission in the Sudan (UNMIS)

DATE: 11 December 2009

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
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*

Internet Service Provide "TS deployment proposal" would remove and separate that traffic. The UN VSAT network would then carry only non-internet data (including voice) circuits. The outcome would be separated services, one solely dedicated to internet thus representing a net increase in bandwidth. As with many Mission projects, the delivery of the solution is often highly dependent on factors outside the control of the Mission. Additionally, CITS believes that the information needs were already identified. The timing of solution delivery was less than ideal. Regarding the single point of failure issue, it was recognized well before the audit and plans to resolve the problem were already in place at the time of the audit. The implementation of the solution, however, required some significant equipment changes. The network redesign is now commonly referred to as UNMIS North & South although full implementation is dependent on works to be carried out at JUBA III site in Juba and the delivery of VSAT infrastructure. Recommendation 5 remains open pending submission to OIOS of documentation showing the complete implementation of the "UNMIS North & South" Project.

D. ICT assets

High rate of personal computer hardware failures

27. A quality management system for the acquisition of reliable equipment is enabled by planning, implementing and maintaining quality controls tests, in accordance with specific quality requirements, procedures and policies. Quality requirements are stated and communicated in quantifiable and verifiable indicators.

28. OIOS noted in the field office location at Juba that a high rate of hardware failures had been registered by the local ICT support staff (mainly failure of hard drives in desktop computers). The cause of such failures was attributed to the environmental conditions in which the equipment was used and operated, and to the inadequacy of an organization-wide ICT standard that did not take into consideration the operational needs of the Mission.

29. Without an adequate ICT quality review process, the Mission is exposed to the risks of failures, rework and increased costs.

Recommendation 6

(6) The UNMIS Communications and Information Technology Section, in coordination with the Field Procurement Section at Headquarters, should review the high rate of hardware failure and propose to the Information and Communications Technology Division at Headquarters the definition of a new ICT standard for the Mission's operations.

30. *The UNMIS Division of Mission Support accepted recommendation 6 and stated that the contract for desktops is a Headquarters systems contract and that UNMIS does not engage in vendor selection. Therefore, questions of*

equipment quality should be best directed to Headquarters. OIOS was informed of the representations the Mission made to Headquarters on the subject of desktop quality and related warranty matters. UNMIS would also like to point out the rates of failure have decreased with the newer models now available under the systems contract. Recommendation 6 remains open pending submission to OIOS of documentation showing the representations made by the Mission to Headquarters on the subject of desktop quality.

E. Project management

Lack of standard project management methodology

31. A standard project management methodology provides a structured approach to document and communicate to relevant stakeholders the critical elements of an initiative. These elements include the objectives that the organization intends to achieve with the implementation of the project, the expected outcomes, necessary resources, responsibilities and implementation timeline. The main benefits from the adoption of a standard methodology is the ability of the organization to assign clear accountabilities, identify benefits, control costs, manage risks and coordinate various activities.

32. OIOS' review found that CITS did not follow a standard project methodology for its locally managed projects, adopting an *ad hoc* approach to the development of each initiative.

33. ICTD has indicated in its draft "vision paper" for the activities in 2009-2010 that the project management methodology to be used for ICT initiatives shall be based on the standard "Project IN Controlled Environment version 2" (PRINCE2).

34. The inconsistent use of a project management methodology could expose the Mission to confusion and uncertainty caused by different approaches within the Organization, and failure to provide adequate control mechanisms and reporting for oversight and monitoring of ICT initiatives, resulting in ineffective and inefficient implementation such as delays and increased costs.

Recommendation 7

(7) The UNMIS Communications and Information Technology Section, in coordination with the Information and Communications Technology Division at Headquarters, should ensure that relevant staff are adequately trained on the project methodology "Project IN Controlled Environment version 2" (PRINCE2), and that any development of future ICT initiatives are in compliance with this standard.

35. *The UNMIS Division of Mission Support accepted recommendation 7 and stated that training on PRINCE2 has been included as part of the ICT training programme for 2009-2010. One ICTS staff member has been selected to*

attend the PRINCE2 training to be held in Entebbe in November 2009. The Mission added that the importance of standard project management methodology is not limited to CITS but to all other sections within UNMIS engaged in projects as CITS does not undertake projects in isolation. Recommendation 7 remains open pending submission from OIOS of documentation showing the completion of the 'PRINCE2' training, and its adoption in the Mission.

F. ICT security management

ICT security risk assessment not implemented

36. The United Nations Secretariat has adopted the professional best practices for the management of ICT security defined in the international standard ISO 27001. DFS has already adopted this standard at the United Nations Logistics Base. In accordance with the ISO standard, an ICT risk management framework should be developed, documenting an agreed-upon level of ICT risks, mitigation strategies and residual risks. Any potential impact on the goals of the mission caused by unplanned events in the ICT operations should be identified, analyzed and assessed. Risk mitigation strategies should be adopted to minimize residual risk to an accepted level. The result of the assessment should be understandable to the stakeholders and if possible, expressed in financial terms, to enable stakeholders to align risk to an acceptable level of tolerance.

37. OIOS found that since CITS does not have a dedicated information security officer post, ICT risk assessments are not conducted. In this condition, UNMIS is unable to identify the risks and their potential impact to its operations, justify the allocation or the request of resources, identify systemic issues and the interdependencies among apparently isolated risks. OIOS therefore reiterates its previous recommendation (AP2006/632/06/04) that periodic ICT risk assessments be performed.

Undocumented ICT security standards

38. The controls required to address the ICT security risks identified through a systematic risk assessment process should be translated into an overall ICT security plan, taking into consideration the specific ICT infrastructure installed at UNMIS. Subsequently, this plan should be supported by documented local security policies and procedures (such as for e-mail and servers), together with appropriate definition of services, responsible officers, software and hardware. The overall ICT security plan should include information security baselines for all major platforms and applications installed at the Mission.

39. No overall ICT security plan, security policies and procedures and e-mail security and server security baselines have been defined at UNMIS. E-mail security and server security configuration settings have not been standardized and formalized at the Mission level.

40. In addition, OIOS noted that since data had not been classified in accordance with the provisions established in ST/SGB/2007/6, potentially

sensitive data on mobile computers was stored insecurely, and no form of encryption (i.e., hard disk encryption) was used to protect these devices.

41. Although CITS referenced general DFS security documentation and had developed drafts of several terms of reference for antivirus, Windows configuration and active directory, Mission-specific security standards had not been documented. In addition, OIOS noted that firewall configuration rules were not adequately documented, and event logging was not properly conducted for both applications and operating systems.

42. OIOS was informed that the Mission intends to develop and implement the necessary procedures once the new post of ICT security officer, requested in its 2009-2010 budget, is finally approved. However, pending the approval of the new budget, CITS should implement compensating controls to ensure that the security requirements and configurations of the network devices are adequately documented and updated on a regular basis. In accordance with the professional best practices adopted by DFS for information security management (ISO 27000 series), CITS should record and safeguard logs of events for Lotus Notes servers (i.e., domino) and databases, client applications, and server operating systems. These logs should include when relevant: (a) user identifiers; (b) dates, times and details of key events (e.g., log-on and log-off); (c) terminal identity or location; (d) records of successful and rejected system access attempts; (e) records of successful and rejected data and other resource access attempts; (f) changes to system configuration; (g) use of privileges; (h) use of system utilities and applications; (i) files accessed and the kind of access; (j) network addresses and protocols; (k) alarms raised by the access control system; (l) activation and deactivation of protection systems (i.e., anti-virus systems and intrusion detection systems).

43. In the absence of properly defined and documented security standards that reflect the specific requirements of the Mission and comprehensive security-related event logs, UNMIS is exposed to the risks of staff members not knowing how to perform critical tasks and not being able to timely investigate, report and correct threats that could affect the continuity of operations and availability of data.

Recommendations 8 to 10

The UNMIS Communications and Information Technology Section should:

(8) Define an overall ICT security plan, security policies and procedures and security baselines at the Mission level. These documents should include: (a) minimum standard security configuration settings for each platform and application installed in the Mission (such as for e-mail and servers); (b) if and where applicable, encryption requirements for “strictly confidential” and “confidential” data; (c) event logging requirements; and (d) an assessment of the confidentiality of data stored on mobile computers and

the implementation of security measures for mobile devices (e.g., hard drive encryption for laptops);

(9) Ensure that systems and network administrators document and review on a regular basis the security configuration of all systems and devices; and

(10) Document the firewall configuration rules and settings and revise them as necessary. In addition, this document should be classified in accordance with the criteria established in ST/SGB/2007/6, on information sensitivity and classification.

44. *The UNMIS Division of Mission Support accepted recommendation 8 and stated that the recruitment of two ICT security staff is underway. Once the new staff members are on board, the matters contained in the recommendation will be evaluated and implemented according to the risk levels applicable to each element. However the classification of data content does not rest with CITS. In cases where business units advise CITS of special security requirements, CITS will undertake specific storage solutions commensurate with the level of security deemed necessary by the business unit.*

45. *Regarding server operations and applications, event logging has always existed. The volume of event-generated transactions can be considerable. Therefore, it is not practical to capture every event capable of being logged. As stated earlier, CITS is not privy to the content of business unit data. Where business units seek special or additional security solutions through extensions to event logging, CITS will respond appropriately. The requirements of each business unit will inevitably be addressed on a case by case basis because each will have differing needs. So as to place the current CITS resource position into perspective, the entire UNMIS server unit now consists of one international staff member. With respect to data encryption, CITS will seek guidance from Headquarters on the standard DFS corporate approach, related corporate license issues and staff resource solutions. However, the decision to encrypt rests with the owner of the data who is ultimately the one best placed to decide on the sensitivity of the data they own or create. The position with respect to desktops (including laptops) remains in place as before, i.e., that no corporate data should be stored there. As to paragraphs 38 to 39 of the audit report, we find these paragraphs to be unfounded as the auditors were given copies of HQ policies on ICT security standards.*

46. OIOS takes note of the comments provided by UNMIS in response to recommendation 8 and further clarifies as follows:

(a) With regard to UNMIS comments that the classification of data content does not rest with CITS and that CITS is not privy to the content of business unit data, OIOS is of the opinion that in accordance with the security requirements established in paragraph 5.4 of ST/SGB/2007/6, both business data owners and CITS should have a proactive role in protecting information. The fact that business unit owners have not

classified their data content nor communicated their security requirements does not mean that sensitive information is not actually collected, processed, transmitted and stored on the ICT infrastructure of UNMIS. This condition is in itself a security risk to the Mission that, within its technical responsibilities and authorities, CITS should mitigate. In fact, CITS is aware that most of the data stored in the Mission's servers and network are the content of applications and systems protected with access control mechanisms. The implementation of these control mechanisms is a clear evidence of the importance given by the business unit managers to protecting the integrity, confidentiality and availability of the data processed with these applications and systems. Therefore, in accordance with the security requirements established in SGB/ST/2007/6 and the professional security standard adopted by DFS (i.e., ISO 27001), CITS should adopt a more secure approach, extending the level of protection granted to the access of data contained in systems and applications, and also to their storage and transmission.

(b) With regard to UNMIS' comments that no corporate data should be stored in desktops and laptops, OIOS is of the opinion that given the nature of mobile computing operations conducted with the use of laptops, these devices are often used to process and store potentially sensitive data, at least temporarily. To prevent the security risks associated with the high rate of stolen or lost devices, and in accordance with paragraph 5.4 of ST/SGB/2007/6, CITS "shall establish procedures to ensure that automated information systems, including networks and telecommunications systems, that collect, create, communicate, compute, disseminate, process or store classified information, have controls that both prevent access by unauthorized persons, and ensure the integrity of the information".

(c) With regard to UNMIS' comments that OIOS' observations in paragraphs 38 to 39 of the present report are unfounded because OIOS was given copies of Headquarters policies on ICT security standards, OIOS wishes to point out that the conditions described in these paragraphs of the present report and the corresponding recommendation (number 8) refer to Mission-specific ICT security plan, policies, and standards related to the local configurations of UNMIS processes and infrastructure, and not, as UNMIS interpreted, to the security standard issued by the Department of Field Support at the Headquarters level.

47. Recommendation 8 remains open pending submission to OIOS of documentation showing the implementation of Mission-specific requirements for: (a) security configuration settings for each platform and application installed in the Mission (such as for e-mail and servers); (b) encryption mechanisms; (c) event logging in accordance with the professional best practices adopted by DFS for information security management (ISO 27000 series) in Lotus Notes Domino, client applications and server operating systems; and (d) security measures for mobile devices (e.g., hard drive encryption for laptops).

48. *The UNMIS Division of Mission Support accepted recommendation 9 and stated that CITS documents and reviews the security configurations of the firewalls and external internet service provider (ISP) routers periodically, including the configuration archive repository for critical network devices on the secure Linux server. Recommendation 9 remains open pending submission to OIOS of a copy of the documented security configuration.*

49. *The UNMIS Division of Mission Support accepted recommendation 10 and stated that firewall configuration rules and settings are documented and revised regularly. CITS will endeavor to classify the documentation in accordance with the criteria established in ST/SGB/200716 on information sensitivity and classification. Recommendation 10 remains open pending submission to OIOS of a classified copy of the firewall configuration rules and settings.*

No vulnerability assessments performed

50. The need to maintain the integrity of information and protect ICT assets requires a security management process. This process also includes performing security monitoring and periodic vulnerability testing, and implementing corrective actions for identified threats, weaknesses or incidents.

51. Although a network intrusion detection system is installed on the UNMIS network, and a limited number of vulnerabilities are detected, periodic vulnerability assessments of the network, servers and applications are not performed systematically.

52. Furthermore, in the absence of a dedicated ICT security officer, the task of periodically performing ICT vulnerability assessments has not been assigned to any other officers.

53. Without a systematic review and assessment of the vulnerabilities of its network, UNMIS is unable to identify security threats and control weaknesses, and to timely implement preventive measures to protect the confidentiality of data and ensure the continuity of operations.

Recommendations 11 and 12

(11) The UNMIS Communications and Information Technology Section should assign the periodic performance of ICT vulnerability assessments to an officer to continuously monitor ICT threats and control weaknesses.

(12) The UNMIS Division of Mission Support should develop and implement a process to ensure that ICT security reports are periodically reported to senior management, and any significant threats are addressed with a remediation plan, defining clear accountability and timeline for its implementation.

54. *The UNMIS Division of Mission Support accepted recommendation 11 and stated that CITS performs vulnerability assessments regularly, based on the open source tools and custom Linux tools in line with the Open Source Security Testing Manual (OSSTM) and ISO 27001 standards. CITS currently targets routers, firewalls, switches and wireless equipment only. The vulnerability assessment for the external internet service provider, routers and firewalls has been concluded and security flaws and vulnerabilities are being addressed. Also implemented is the operational demilitarized zone concept for servers. This will be further enhanced when the two ICT security staff currently under recruitment are on board. Recommendation 11 remains open pending submission to OIOS of copies of the reports generated during the last year as a result of the vulnerability assessments performed in accordance with OSSTM and ISO 27001 standards.*

55. *The UNMIS Division of Mission Support accepted recommendation 12 and stated that this recommendation is pending the recruitment of two ICT security staff, which is underway. Security reports to senior management will be among the duties to be performed. Recommendation 12 remains open pending submission to OIOS of copies of the ICT security reports provided to senior management.*

Inadequate network security

56. Sensitive data should only be exchanged over a trusted path or medium with controls to provide data integrity and confidentiality.

57. OIOS noted insecure (i.e., not encrypted) network traffic within the Mission, such as network traffic between Khartoum, the sectors and the team sites. For instance, the use of Telnet and FTP protocols exposed highly confidential user credentials (user names and passwords).

58. In addition, microwave and VSAT links transmitted critical data in an unprotected manner (e.g., e-mail, Lotus Notes databases used by substantive offices, VIPs' link to the intranet and remote maintenance of network devices). Furthermore, OIOS identified unencrypted remote desktop connections to critical servers located in the network.

59. An inadequate level of network security exposes the Mission to potential risks associated with the breach of confidentiality and integrity of sensitive data, security breaches not detected in a timely manner and unauthorized access to systems and applications.

Recommendations 13 and 14

(13) The UNMIS Division of Mission Support should replace all insecure network services, including the insecure remote desktop connections, with remote connectivity security solutions.

(14) The UNMIS Communications and Information Technology Section should extend the Virtual Private

Network connectivity solution already adopted for e-mail replication to the replication process of all critical Lotus Notes databases.

60. *The UNMIS Division of Mission Support did not accept recommendation 13 and stated that it cannot accept the claim that UNMIS network has inadequate network security from the evidence presented in the audit report. CITS does not believe it is practical to encrypt all network services. The proposition that Telnet and FTP is a security exposure depends entirely on what is actually being transmitted in the first place. UNMIS does not accept the inference that Telnet and FTP of themselves constitute evidence of an insecure UNMIS network, but is prepared to accept that in the case of Telnet, where alternative options are available, these should (and will) be used by CITS.*

61. OIOS is unable to accept the assertions made by UNMIS and reiterates that the security of the Missions' network is inadequate, on the basis of the following observations:

(a) As acknowledged by UNMIS, the Mission did not classify its information in accordance with the requirements established in ST/SGB/2007/6 on information sensitivity, classification and handling. Therefore, CITS is not able to determine where and when sensitive data have been transmitted in its network. Since UNMIS used unprotected (unencrypted) means of data communication this condition exposed potentially sensitive data to serious risks to their confidentiality and integrity. The relevance of these risks is compounded by the lack of systematic information security risk assessments in the Mission, already reported in paragraphs 36 and 37 of the present report;

(b) As a consequence of the condition described in the preceding point, UNMIS' use of unprotected (unencrypted) means of data communication is contrary to the security requirements established in paragraph 5.4 of ST/SGB/2007/6;

(c) Furthermore, UNMIS' use of unprotected (unencrypted) means of data communication disregards the security principle established in the DPKO/DFS official standard operating procedure (Ref. 2009.12) on File Transfer Protocol (FTP), which stated that "FTP is an inherently insecure file transfer method as no encrypted transfer method is specified. This means that under most network configurations, user name, passwords, FTP commands and transferred files can be 'sniffed' or viewed by anyone on the same network using a packet sniffer";

(d) In addition, UNMIS' use of unprotected (unencrypted) means of data communication is also not in compliance with the information security management standard (ISO 27001) adopted by DFS.

62. OIOS therefore reiterates recommendation 13, which will remain open pending reconsideration by UNMIS of its initial position on the matter and

submission to OIOS of documentation showing that all insecure (i.e., unencrypted) protocols have been replaced with security solutions.

63. *The UNMIS Division of Mission Support did not accept recommendation 14 and stated that VPN encryption of mail replication is limited to insecure circuits which CITS regards as being point to point transmissions through the internet, etc. CITS also encrypts all UN traffic through third party leased lines. While the Notes-based telephone directory might be seen as critical, CITS has no plans at this point to encrypt the replication of it through the UNMIS UN network. However, where a database contains sensitive confidential data (even where that data is being replicated through a UN Microwave or UN VSAT transmission), CITS is prepared to encrypt if the business unit owner (who manages data content) indicated the need to do so. CITS will also endeavor to reaffirm (with the business owners) what their security requirements are when the CITS IT Security staff members are recruited. Subject to guidance from HQ, at this stage UNMIS does not intend to implement generalized encryption of all UN VSAT data transmissions between UNMIS HQ and the Sector HQs.*

64. OIOS wishes to stress that the Mission's data is exposed to serious security risks because: (a) UNMIS did not classify its information in accordance with ST/SGB/2007/6; (b) CITS is unable to determine when and where sensitive data is transmitted; (c) CITS did not conduct any risk assessment to identify potential information security risks; and (d) CITS did not protect its data transmission links with encryption mechanisms. OIOS is of the opinion that while business unit owners have not classified their information, this does not justify CITS' decision to support the transmission of information with unprotected means of communication. The security principles established in ST/SGB/2007/6 and professional standards (i.e., ISO 27001) should have guided CITS in adopting a more secure approach, since the data transmitted during the replication process pertained to the content of Lotus Notes databases protected with access control mechanisms that require the authentication of users with unique credentials (user identification and passwords). Therefore, the same protection granted to the access of data contained in the Lotus Notes databases should have also been extended to its transmission (i.e., replication via UNMIS microwave or satellite links), using protected means of communication (ST/SGB/2007/6, Section 5 f). OIOS therefore reiterates recommendation 14, which will remain open pending reconsideration by UNMIS of its initial position on the matter and submission to OIOS of documentation showing that secure (encrypted) means of communication have been implemented for the replication of all Lotus Notes databases installed in the Mission.

Inadequate access control and insecure transmission of data sent through digital senders

65. Access control procedures to official applications and devices should include the use of unique identifiers (i.e., personal identification number or PIN) to enable users to be linked to and held accountable for their actions. The use of unique user identifiers also enforces a check that the user has authorization from the system owner for the use of the information service and that the access is appropriate to the business purpose and consistent with the organizational

security policy. In addition, in accordance with ST/SGB/2007/6, sensitive information should be transmitted through secure (i.e., encrypted) means of communications.

66. UNMIS installed 148 digital senders in 29 locations throughout the Mission. Although policies and procedures existed to control devices connected to the network, the digital senders did not require users to authenticate themselves in order to send images of documents. This condition resulted in several cases of misuse reported to the UNMIS Conduct and Discipline Unit, whereby inappropriate documents had been sent through the digital senders. Furthermore, the transmission of documents sent through the digital senders was in clear text (not encrypted), exposing the content of potentially sensitive information to the risk of being intercepted and subsequent unauthorized access.

67. OIOS reviewed the technical specifications of the digital senders installed in UNMIS and identified that the following mitigating controls can be configured on the devices:

(a) User authentication: The digital senders can be configured with several authentication mechanisms, (i.e. Personal Identification Numbers (PINs); Lightweight Directory Authentication Protocol (LDAP); and Kerberos authentication; and

(b) Security of data transmission: The transmission of data sent through the digital senders can be performed using secure protocols (i.e. Secure Socket Layer "SSL", or Internet Protocol Security IPsec), or a secure e-mail option based on a secondary e-mail feature designed to work with third-party software programs that encrypt the data between the device and the server. In alternative, other mitigating measures could be implemented by blocking the directory of users, and prevent the transmission of documents outside the internal "trusted" domain, or configure the firewalls with a specific rule filtering the (internet protocol "IP") address of the digital senders.

Recommendation 15

(15) The UNMIS Division of Mission Support should review the security policy and settings of the digital senders installed to ensure users' authentication and integrity of data transmitted by configuring them with the following protective measures: (a) authenticating every user of the device by requiring unique credentials (i.e., using personal identification numbers); and (b) protecting the transmission of data sent with the device using secure protocols (e.g., Secure Socket Layer (SSL), Internet Protocol Security IPsec; and secondary e-mail features).

68. *The UNMIS Division of Mission Support did not accept recommendation 15 but stated that the observation that users of digital senders can send scanned images without being personally identified via login authentication is correct.*

However, the use of digital senders is limited to sending scanned images and the additional overheads in logging-in every time a user wants to send an image is unlikely to generate much enthusiasm among the users, the digital sender being a widely shared device. Furthermore, user authentication is not going to prevent non-work related use of the digital sender. CITS is not aware of numerically significant instances where digital sender user anonymity has presented problems. Also, there are numerous ways in which anonymous document transmissions can be undertaken. Nonetheless, the two ICT security posts will be assigned the responsibility for monitoring the frequency of all abuses (including transmission via digital senders). If digital senders prove to be singularly problematic, additional security measures will be considered, as appropriate.

69. OIOS is unable to accept the assertions made provided by the UNMIS Division of Mission Support, and clarifies that:

(a) With regard to UNMIS' comment that the use of digital senders is limited to sending scanned images, OIOS is of the opinion that scanned images can include sensitive documents that in accordance with ST/SGB/2007/6, Section 5 f, should be transmitted with secure means of communication; and

(b) With regard to UNMIS' comment that user authentication is not going to prevent non-work related use of a sender, OIOS is of the opinion that the authentication mechanisms will discourage potentially inappropriate use of the digital senders.

70. OIOS therefore reiterates recommendation 15, which will remain open pending reconsideration by UNMIS of its initial position on the matter and submission to OIOS of documentation showing that user authentication mechanisms and data transmission protection have been implemented for the use of digital senders.

Disaster recovery and business continuity (DRBC) for ICT operations still in draft form

71. Documented and tested procedures for DRBC are a critical element of peacekeeping operations. In this regard, UNMIS has developed and implemented relevant controls, such as:

(a) The UNMIS Disaster Recovery Plan for Mission Communications and IT Systems, Draft Version 1, dated 20 November 2007. To date, however, the plan is still in draft;

(b) The process simulation of disaster and requirements for minimization of impact to CITS services, dated 18 February 2008;

(c) The formal memo issued by the Director of Mission Support, dated 12 March 2008, for the identification of sections' focal points to ensure the implementation of a comprehensive Mission DRBC plan;

(d) The overview of UNMIS IT DRBC, dated August 2008, defining three broad levels at which IT attempts to address data and system restoration;

-
- (e) The draft "CITS Contingency Plan and What If Scenario", not dated; and
 - (f) The Sudan emergency communication system, not dated.

72. OIOS was informed of the ongoing process for the establishment of a shared disaster recovery facility in Entebbe that will serve as a multi-mission regional DRBC site.

Recommendation 16

(16) The UNMIS Division of Mission Support should update and formally issue the disaster recovery and business continuity plans for information and communications technology operations drafted in November 2007.

73. *The UNMIS Division of Mission Support accepted recommendation 18 and stated that the updating of the DRBC plan is an ongoing process. UNMIS plans to implement the recommendation when the next critical milestone is reached, i.e., testing by the business continuity users. Input from clients is required in order to determine their critical business functions and where they will be carried out under a range of possible disaster situations. This would confirm that the disaster recovery infrastructure is capable of delivering a business continuity solution.* Recommendation 18 remains open pending submission to OIOS of documentation showing the results of the testing performed by business continuity users, and the updated version of the DRBC plan for ICT operations.

G. Status of previous audit recommendations

74. The implementation of eight of the 20 OIOS' audit recommendations issued in the previous audit report on the management of ICT at UNMIS (AP2006/632/06, dated 25 October 2007), was still pending. These recommendations included:

- (a) Issuance of standard operating procedures for the receipt, issue and disposal of assets (AP2006/632/06/001; high risk recommendation);
- (b) Performance of periodic ICT risk assessments (AP2006/632/06/004; high risk recommendation);
- (c) Development of a Mission-specific ICT security policy (AP2006/632/06/005);
- (d) Development of a Mission-specific disaster recovery and business continuity plan (AP2006/632/06/06; high risk recommendation);
- (e) Training of CITS staff on information security, and the use of CIT equipment and systems (AP2006/632/06/014);
- (f) Establishment of the Information and Communications Technology Review Committee (AP2006/632/06/015); and
- (g) Creation of the Information and Communications Technology Security Unit (AP2006/632/06/018).

75. The UNMIS Division of Mission Support needs to ensure the timely implementation of all pending audit recommendations, with particular attention to those designated as high risk. *The UNMIS Division of Mission Support stated that six recommendations related to OIOS' audit report AP2006/632/06, have been already implemented.* With regard to recommendation AP2006/632/06/07, UNMIS stated that *CITS had given the proposed training course content to the Integrated Mission Training Centre, which coordinates and conducts training for the Mission. CITS will also provide OIOS with a copy of a Headquarters-developed Power Point presentation that covers the core issues and this is targeted at new staff, for possible incorporation in future training schedule.* In order for OIOS to close these recommendations, OIOS requests that the Mission provide documentation showing their implementation.

V. ACKNOWLEDGEMENT

76. 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.

STATUS OF AUDIT RECOMMENDATIONS

Recom. no.	Recommendation	Risk category	Risk rating	C/O	Actions needed to close recommendation	Implementation date ²
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.	Human Resources	Medium	O	Provide evidence documenting the actions taken to recruit staff specialized in ICT security-related disciplines.	Not provided
2	The UNMIS Division of Mission Support should ensure that all units in the Communications and Information Technology Section develop and communicate a work plan based on a standardized structure.	Governance	Medium	O	Provide documented evidence that standard work plans have been developed and communicated to all staff in CITS.	Not provided
3	The UNMIS Division of Mission Support should 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.	Governance	Medium	O	Provide evidence documenting established and functioning procedures to systematically monitor the implementation of ICT work plans, with defined performance indicators, a reporting schedule, and a process to promptly act upon deviations.	Not provided
4	The UNMIS Division of Mission Support should review, update and formalize all policies, standard operating procedures and guidelines related to ICT operations.	Governance	Medium	O	Provide copy of the finalized policies, standard operating procedures, and guidelines related to ICT operations.	Not provided
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.	Operational	Medium	O	Provide documented evidence of the complete implementation of the "UNMIS North & South" Project.	Not provided
6	The UNMIS Communications and Information Technology Section, in coordination with the Field Procurement	Operational	Medium	O	Provide evidence documenting the representations made by the Mission to HQ on the subject of PC quality.	Not provided

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
7	<p>Section at Headquarters, should review the high rate of hardware failure and propose to the Information and Communications Technology Division at Headquarters the definition of a new ICT standard for the Mission's operations.</p> <p>The UNMIS Communications and Information Technology Section, in coordination with the Information and Communications Technology Division at Headquarters, should ensure that relevant staff are adequately trained on the project methodology "Project IN Controlled Environment version 2" (PRINCE2), and that any development of future ICT initiatives are in compliance with this standard.</p>	Human Resources	Medium	O	Provide documented evidence about the completion of the 'PRINCE2' training, and its adoption in the Mission.	Not provided
8	<p>The UNMIS Communications and Information Technology Section should define an overall ICT security plan, security policies and procedures and security baselines at the Mission level. These documents should include: (a) minimum standard security configuration settings for each platform and application installed in the Mission (such as for e-mail and servers); (b) if and where applicable, encryption requirements for "strictly confidential" and "confidential" data; (c) event logging requirements; and (d) an assessment of the confidentiality of data stored on mobile computers and the implementation of security measures for mobile devices (e.g., hard drive encryption for laptops).</p>	Governance	High	O	Provide evidence documenting the implementation of Mission-specific requirements for: a) security configuration settings for each platform and application installed in the Mission (such as for e-mail and servers); b) encryption mechanisms; c) event logging in accordance with the professional best practices adopted by DFS for information security management (ISO 27000 series) in Lotus Notes Domino, client applications, and server operating systems; and d) security measures for mobile devices (e.g. hard-drive encryption for laptops).	Not provided
9	The UNMIS Communications and Information Technology Section should	Operational	Medium	O	Provide documented evidence of the security configuration prepared by systems	Not provided

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
10	<p>ensure that systems and network administrators document and review on a regular basis the security configuration of all systems and devices</p> <p>The UNMIS Communications and Information Technology Section should document the firewall configuration rules and settings and revise them as necessary. In addition, this document should be classified in accordance with the criteria established in ST/SGB/2007/6, on information sensitivity and classification.</p>	Operational	Medium	O	<p>and network administrators.</p> <p>Provide classified copy of the firewall configuration rules and settings.</p>	Not provided
11	<p>The UNMIS Communications and Information Technology Section should assign the periodic performance of ICT vulnerability assessments to an officer to continuously monitor ICT threats and control weaknesses.</p>	Operational	High	O	<p>Provide copies of the reports generated during the last year as a result of the vulnerability assessments performed in accordance with OSSTM and ISO 27001 standards.</p>	Not provided
12	<p>The UNMIS Division of Mission Support should develop and implement a process to ensure that ICT security reports are periodically reported to senior management, and any significant threats are addressed with a remediation plan, defining clear accountability and timeline for its implementation.</p>	Governance	Medium	O	<p>Provide ICT security reports reported to senior management.</p>	Not provided
13	<p>The UNMIS Division of Mission Support should replace all insecure network services, including the insecure remote desktop connections, with remote connectivity security solutions.</p>	Operational	High	O	<p>Provide documented evidence demonstrating that all insecure (i.e. un-encrypted protocols) have been replaced with security solutions.</p>	Not provided
14	<p>The UNMIS Communications and Information Technology Section should extend the Virtual Private Network connectivity solution already adopted for e-mail replication to the replication process of all critical Lotus Notes databases.</p>	Operational	Medium	O	<p>Provide documented evidence demonstrating that secure means (encrypted) of communications have been implemented for the replications of all Lotus Notes databases installed in the Mission.</p>	Not provided

Recom. no.	Recommendation	Risk category	Risk rating	C/ ¹ O ¹	Actions needed to close recommendation	Implementation date ²
15	The UNMIS Division of Mission Support should review the security policy and settings of the digital senders installed to ensure users' authentication and integrity of data transmitted by configuring them with the following protective measures: (a) authenticating every user of the device by requiring unique credentials (i.e., using personal identification numbers); and (b) protecting the transmission of data sent with the device using secure protocols (e.g., Secure Socket Layer (SSL), Internet Protocol Security IPsec; and secondary e-mail features).	Operational	Medium	O	Provide evidence documenting that user authentication mechanisms and data transmission protection have been implemented for the use of digital senders	Not provided
16	The UNMIS Division of Mission Support should update and formally issue the disaster recovery and business continuity plans for information and communications technology operations drafted in November 2007.	Governance	High	O	Provide copies of the results of the testing of business continuity users, complete with the updated version of the disaster recovery and continuity plans for ICT operations.	Not provided

¹ C = closed, O = open

² Date provided by UNMIS in response to recommendations