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. Edmond Mulet, Special Representative of the Secretary-General and Head of Mission
A: United Nations Stabilization Mission to Haiti

DATE: 27 September 2010

REFERENCE: IAD: 10- 00820

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

SUBJECT: **Assignment No. AT2009/683/01 – Audit of information and communications technology governance and security management in MINUSTAH**
OBJET:

Additional controls must be implemented to ensure adequate support for business continuity and disaster recovery, and to mitigate risks to information security

1. I am pleased to present the report on the above-mentioned audit which was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

2. Based on your comments, we are pleased to inform you that we will close recommendation 8 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 high risk (i.e., recommendations 1 and 2), in its annual report to the General Assembly and semi-annual report to the Secretary-General.

EXECUTIVE SUMMARY

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

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

The audit found that MINUSTAH had already designed and implemented several controls for strengthening of its ICT operations. However, there were several controls that require adequate attention by Management. These include:

a) Completion of the business continuity plan with defined procedures for all processes;

b) Improvement to the physical security of the disaster recovery site in Santo Domingo;

c) Formalizing and implementing incident and change management processes;

d) Mitigating the risks identified in the security of data and network with the implementation of controls for the review of access rights, password management, and wireless and laptop security; and

e) Increasing staff awareness for the protection of information resources.

I. INTRODUCTION

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

2. The Communications and Information Technology Section provides the following support services in MINUSTAH:

Information technology**:**

(a) Provision of support to and maintenance of 106 servers, 2,416 desktop computers, 874 laptop computers, 618 printers and 181 digital senders;

(b) Provision of support to and maintenance of local-area networks (LAN) and wide-area networks (WAN) for an average of 3,700 users.

Communications:

(c) Provision of support to and maintenance of a satellite network consisting of 2 Earth station hubs and 23 very small aperture terminal (VSAT) systems (9 in Port-au-Prince and 14 in remote locations) to provide voice, fax, video, data communications, disaster recovery and business continuity services;

(d) Provision of support to and maintenance of 31 telephone exchanges and 138 microwave links;

(e) Provision of support to and maintenance of the ultra-high frequency (UHF) repeater network consisting of 3,469 hand-held radios, 1,239 mobile radios, 115 base station radios, 2,129 hand-held radios trunking, 650 mobile radios trunking and 80 trunking base station radios;

(f) Provision of support to and maintenance of the high frequency (HF) network consisting of 1,121 mobile radios with a global positioning system option and 107 data-capable base stations;

(g) Provision of support to and maintenance of 13 communications centres; and

(h) Provision of support to and maintenance of 25 communications sites to enhance microwave and ultra-high frequency network coverage throughout Haiti.

3. The financial resources for information and communications in the recent budget cycles are as follows:

(Thousands of United States dollars. Budget year is 1 July to 30 June)

	Expenditures (2007/08) (1)	*Apportionment (2008/09) (2)*	*Cost estimates (2009/2010) (3)*	*Amount (4)=(3)-(2)*	*Percentage (5)=(4)/(2)*
Information technology	5,455.5	7,168.0	7,441.3	272.2	3.8
Communications	23,059.8	24,584.8	26,089.1	1,504.3	6.1

4. Comments made by MINUSTAH 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.

III. AUDIT SCOPE AND METHODOLOGY

6. Interviews were held with representatives from the Communications and Information Technology Section (CITS), support and substantive offices in Port-au-Prince. 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. A site visit was conducted to the disaster recovery and business continuity location in Santo Domingo.

IV. AUDIT FINDINGS AND RECOMMENDATIONS

A. Business continuity planning

7. A business continuity plan should identify potential threats to the Mission, the potential impact that those threats, if realized, might cause, and formulate a response to safeguard assets and ensure continuity of operations.

8. OIOS reviewed the latest version (ver. 2.2) of the business continuity and disaster recovery plan developed in MINUSTAH in September 2008. The plan included the following provisions and scenarios:

(a) Supported locations;

(b) Operational tiers;

(c) Technical infrastructure and ICT services;

(d) Roles;

(e) Impact analysis and scenarios; and

(f) Testing.

9. While the plan contained adequate information and provisions with regard to the technical aspects of the business continuity and disaster recovery, no details were provided on the critical business processes to be followed by each office to ensure prompt recovery of data and continuity of operations. MINUSTAH also needs to document the lessons learned during the recent earthquake in Haiti, in regard to business continuity and disaster recovery.

10. Additionally, MINUSTAH established a business continuity and disaster recovery plan in the building of the United Nations International Research and Training Institute for the Advancement of Women (INSTRAW) in Santo Domingo. OIOS' visit to this location showed that the server room hosting all the replicated data presented major physical controls weaknesses, such as inadequate protective door, fire and water protection, and alarms.

Recommendations 1 to 3

(3) The MINUSTAH Communications and Information Technology Section should document the lessons learned during the recent earthquake to ensure continuity of communications and the availability of information resources.

(2) The MINUSTAH Division of Mission Support should document a business impact analysis and continuity plan in line with the guidelines established by the United Nations Secretariat.

(3) The MINUSTAH Division of Mission Support should implement measures to address the physical security weaknesses of the server room in the INSTRAW building in Santo Domingo.

11. *MINUSTAH concurred with recommendation 1 and indicated that the Best Practices Unit organized several meetings with representatives of all MINUSTAH Sections, including CITS. in order to gather information pertaining to lessons learnt. While the Mission awaits the finalization of that report, the CITS has been instructed to prepare a report of lessons learned. Once completed it will be shared with OIOS.* Recommendation 1 remains open pending receipt of the documented lessons learned in the Mission with regard to the continuity of communications and availability of information resources.

12. *MINUSTAH concurred with recommendation 2 and indicated that the Mission Support Division will endeavor to implement a business continuity plan. The Mission further noted that an exercise was held where key personnel from various sections were physically brought to Santo Domingo to test systems in the event business has to be relocated there.* Recommendation 2 remains open pending receipt of the documented business impact analysis and continuity plan.

13. MINUSTAH accepted recommendation 3 and indicated that the Mission has installed CCTV cameras in the INSTRAW office. In addition, the implementation of an access cards system will start the first week of May and its expected completion date is 10 May 2010. Access will only be granted to CITS staff. Recommendation 3 remains open pending receipt of the documented evidence that the CCTV system and access cards reader in the INSTRAW office was implemented.

B. Incident and change management procedures

14. Incident and change management procedures should define reporting and escalation procedures that staff, contractors, and third party users must follow to ensure adequate and timely communication and follow-up of events (including changes) that could have an impact on the security of organizational assets and operations.

15. MINUSTAH developed standard operating procedures for both incident and change management, as follows:

(a) The incident management procedure (draft version, dated February 2010) detailed a workflow of the process, the prioritization criteria, and the steps to be followed for initiation, classification, initial support, investigation and analysis, and resolution. For these procedures, however, OIOS was not able to identify clear evidence confirming their implementation; and

(b) The change management procedure (version dated August 2007) documented roles, workflow, and types of requests, including details of the automated system (Lotus Notes database) used for managing the process. While the procedure provided detailed step-by-step instructions for processing changes, OIOS noted that there were no provisions indicating who would handle emergency changes, and how. Given that the nature of threats to which the Mission is exposed often has an emergency connotation, the unavailability of ad-hoc provisions for processing these changes could prevent the Mission from adequately resolving time-sensitive tasks.

Recommendations 4 to 5

(4) The MINUSTAH Communications and Information Technology Section should implement the incident management procedure and document any lessons learned from the tasks performed after the earthquake.

(5) The MINUSTAH Communications and Information Technology Section should complete the change management procedure with ad-hoc instructions documenting the handling of emergency changes.

16. *MINUSTAH accepted recommendation 4 and indicated that CITS is governed by the ICTD issued policy on this matter. In this regard, the Mission provided copy of the working draft policy directive developed by DPKO/DFS on incident management.* Recommendation 4 remains open pending receipt of the formally approved policy directive developed by DPKO/DFS for incident management.

17. *MINUSTAH accepted recommendation 5 and indicated that ad-hoc emergency situations do not in any case affect change management procedures. Even in emergency situations, change management is always planned and has to be performed in accordance with the clear guidelines issued by ICTD.* OIOS was provided a copy of the approved SOP since August 2007, which shows the relevant work already done by the Mission in preparing its change management (SOP 3/14). However, OIOS noted that this SOP addressed changes only for "normal" operations. ICTD has adopted the information security management standard ISO 27001, defining the following requirements (14.1.4) for change management procedures: "Procedures should be included within the Organization's change management programme to ensure that business continuity matters are always addressed appropriately…..including emergency procedures, manual fallback plans, and resumptions plans". Recommendation 5 remains open pending receipt of an updated change management procedure containing instructions for emergency changes.

C. Security

Network security

18. Best practices in the field of information security require the segregation of internal and external local area networks.

19. OIOS identified that the wireless network (802.11 Wi-Fi Access Points) located around the MINUSTAH Log Base site (including the data centers) were not segmented from the internal local area network, thereby increasing the risk of compromise of the internal network in the event any of the wireless access points is breached. This weakness could result in unauthorized access to MINUSTAH information systems and information resources resulting in loss of confidentiality, integrity and availability of information assets.

Recommendation 6

(6) The MINUSTAH Communications and Information Technology Section should configure the wireless (Wi-Fi) access points

in a separate network segment (i.e. virtual local area network) outside of the internal network, and filter traffic between this network segment and the internal network.

20. *MINUSTAH accepted recommendation 6 and indicated that wireless access points are segmented onto the separate VLAN and access is controlled (by WPA-PSK) as an additional security measure. MINUSTAH domain authentication is implemented for the wireless access. Traffic filtering implementation is pending the arrival of the NeiFlow software, which is still under procurement process.* Recommendation 6 remains open pending receipt of documentation confirming that traffic filtering between network segments and the internal network has been implemented.

Mobile security

21. The use of mobile computing devices offers advantages in terms of flexibility and convenience of use. However, the risks of loss and theft of these devices is statistically significant. Therefore, best practices require that mobile computers (i.e. laptops) are protected - in addition to access controls – with data encryption mechanisms that would prevent breaches to the confidentiality of data in case of loss or stolen devices.

22. The policy established in MINUSTAH stipulated that each portable device is owned by its respective division/office and the responsibillity for maintaining such devices, including their security, rests with each division/office. OIOS found that the laptops used in the Mission, containing sensitive information, were not encrypted. Therefore, the sensitive information stored in these mobile devices was exposed to a significant risk in case of loss or theft.

Recommendation 7

(7) The MINUSTAH Communications and Information Technology Section should implement more stringent security measures for laptops by configuring them with hard-drive and removable media encryption.

23. *MINUSTAH concurred with recommendation 5 and indicated CITS has already identified the acceptable product that could support encryption of hard drives and removable medias on laptops, however the cost of this software exceeds` $200,000, which is more that the total annual budget allotment for the acquisition and renewal of software packages ($107.000). Given the seriousness of the situation, the Mission will approach ICTD for advice and further action.* Recommendation 7 remains open pending receipt of the mitigating measures implemented by CITS in coordination with ICTD for the encryption of mobile computing devices.

Access security

24. Access to systems and networks should be protected with policies and mechanisms to ensure that only authorized staff can access data and resources on a need-to-know basis.

25. OIOS conducted a review of the user accounts and access control mechanisms configured in the Mission for managing servers, network, and applications. The results of this review indicated that:

(a) A mechanism to force selection of strong passwords was not currently in place on all production servers;

(b) There were no mechanisms in place for enforcing the selection of strong passwords by users;

(c) Certain accounts (i.e. Microsoft SQL accounts) had blank passwords on the Blackberry enterprise and billing servers;

(d) There was no consistency in enforcing regular password changes for users (42 days) and administrators (30 days), with the following statistics:

- Accounts found = 8,421
- Accounts with password not changed in past 42 days = 3,018 (35%)
- Accounts with password not changed in past 90 days = 2,614 (30%)
- Accounts with password not changed over 1 year ago = 1,278 (15%)
- Accounts with password not changed over 2 years ago = 378 (0.04%)
- Accounts with password not changed over 3 years ago = 174 (0.02%)
- Accounts with password not changed over 4 years ago = 20 (0.002%)
- AD Accounts with password not changed over 5 years ago = 8 (0.0009%).

Recommendation 8

(8) The MINUSTAH Communications and Information Technology Section should implement mechanisms to enforce selection of strong passwords on all operating systems and applications and then develop and implement an adequate awareness programme to make users aware of this requirement. In particular, it should be ensured that:

(a) Users change passwords every 42 days on all servers;

(b) Administrators change passwords every 30 days on all servers; and

(c) Users and administrators select strong passwords consisting of numbers, different case characters and symbols.

26. *MINUSTAH accepted recommendation 8 and indicated that the mechanism for the implementation of these observations is in place, and that a policy document on password management was created and distributed to all MINUSTAH staff on the 13 October 2009 via Bulletin Board (Annex-Il). All network accounts are currently prompted to change passwords every 42 days. Administrator passwords are prompted to be changed every 30 days.* Based on the actions taken by the Mission and the documentation provided, OIOS will close recommendation 8.

V. ACKNOWLEDGEMENT

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

cc: 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

CONTACT INFORMATION:

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

DEPUTY DIRECTOR:
Gurpur Kumar: Tel: +1.212.963.5920, Fax: +1.212.963.3388,
e-mail: kumar@un.org

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

ANNEX 1

STATUS OF AUDIT RECOMMENDATIONS

Recom. no.	Recommendation	Risk category	Risk rating	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
1	The MINUSTAH Communications and Information Technology Section should document the lessons learned during the recent earthquake to ensure continuity of communications and the availability of information resources.	Information Resources	High	O	Document lessons learned in the Mission with regard to the continuity of communications and availability of information resources	2 quarter 2010
2	The MINUSTAH Division of Mission Support should document a business impact analysis and continuity plan in line with the guidelines established by the United Nations Secretariat.	Information Resources	High	O	Document business impact analysis and continuity plan.	Not provided
3	The MINUSTAH Division of Mission Support should implement measures to address the physical security weaknesses of the server room in the INSTRAW building in Santo Domingo.	Information Resources	Medium	O	Implement the CCTV system and access cards reader in the INSTRAW office was implemented.	2 quarter 2010
4	The MINUSTAH Communications and Information Technology Section should implement the incident management procedure and document any lessons learned from the tasks performed after the earthquake.	Information Resources	Medium	O	Formal issuance of the policy directive developed by DPKO/DFS for incident management.	Not provided
5	The MINUSTAH Communications and Information Technology Section should complete the change management procedure with ad-hoc instructions documenting the handling of emergency changes.	Information Resources	Medium	O	Update the change management procedure containing ad-hoc instructions for emergency changes.	Not provided

Recom. no.	Recommendation	Risk category	Risk rating	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
6	The MINUSTAH Communications and Information Technology Section should configure the wireless (Wi-Fi) access points in a separate network segment (i.e. virtual local area network) outside of the internal network, and filter traffic between this network segment and the internal network.	Information Resources	Medium	O	Implement the traffic filtering between network segments and the internal network has been implemented.	Not provided
7	The MINUSTAH Communications and Information Technology Section should implement more stringent security measures for laptops by configuring them with hard-drive and removable media encryption.	Information Resources	Medium	O	Implement mitigating measures in coordination with ICTD for the encryption of mobile computing devices.	Not provided
8	The MINUSTAH Communications and Information Technology Section should implement mechanisms to enforce selection of strong passwords on all operating systems and applications and then develop and implement an adequate awareness programme to make users aware of this requirement. In particular, it should be ensured that: (a) Users change passwords every 42 days on all servers; (b) Administrators change passwords every 30 days on all servers; and (d) Users and administrators select strong passwords consisting of numbers, different case characters and symbols.	Information Resources	Medium	C		Implemented

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