Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2014/130

Audit of information and communications technology security in the United Nations Support Office for the African Union Mission in Somalia

Overall results relating to effective management of information and communications technology security were initially assessed as partially satisfactory. Implementation of four important recommendations remains in progress.

FINAL OVERALL RATING: PARTIALLY SATISFACTORY

10 December 2014
Assignment No. AT2014/638/02

CONTENTS

AUDIT REPORT

Audit of information and communications technology security in the United Nations Support Office for the African Union Mission in Somalia

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of the information and communications technology (ICT) security in the United Nations Support Office for the African Union Mission in Somalia (UNSOA).

2. In accordance with its mandate, OIOS provides assurance and advice on the adequacy and effectiveness of the United Nations internal control system, the primary objectives of which are to ensure: (a) efficient and effective operations; (b) accurate financial and operational reporting; (c) safeguarding of assets; and (d) compliance with mandates, regulations rules.

3. UNSOA provides logistical support to the African Union Mission in Somalia (AMISOM); the United Nations Assistance Mission in Somalia (UNSOM); the Office of the Special Envoy of the Secretary General for the Great Lakes Region (O/SESG-GLR) in Nairobi; and the Somalia-Eritrea Monitoring Group (SEMG). UNSOA also provides Umoja support and performs transactions for UNSOM, O/SESG-GLR and SEMG.

4. The 2013/2014 budget of UNSOA was $434 million, with 241 international and 160 national staff in support of an authorized strength of 22,126 AMISOM troops, 260 individual police officers, 280 formed police personnel, 70 AMISOM civilian staff and 10,900 Somalia National Army troops.

5. The Information and Communications Technology Section (ICTS) of UNSOA supported 26 very small aperture terminal systems (VSAT), 19 microwave links, four containerized modular data centres, 18 communication containers, 3 mobile deployable telecommunications systems (MDTS), 28 physical servers, 250 virtual servers, 237 desktop computers and thin clients, 511 laptop computers, 62 printers, 11 wide area networks and 9 local area networks in nine locations to support United Nations and AMISOM personnel. In addition, ICTS supported the ICT infrastructure in Mogadishu to enable UNSOA to remotely support AMISOM in-theatre operations, and maintained 1,070 e-mail accounts of UNSOA, UNSOM, AMISOM, SESG-GLR, SEMG personnel.

6. Comments provided by UNSOA are incorporated in italics.

II. OBJECTIVE AND SCOPE

7. The audit was conducted to assess the adequacy and effectiveness of UNSOA governance, risk management and control processes in providing reasonable assurance regarding the **effective management of ICT security in UNSOA**.

8. This audit was included in the OIOS work plan for 2014 because of the high risks associated with the ICT security in UNSOA.

9. The key controls tested for the audit were: (i) Risk assessment; and (ii) ICT support systems. For the purpose of this audit, OIOS defined these key controls as follows:

(a) **Risk assessment** – controls that provide reasonable assurance that risks relating to ICT security in UNSOA are identified and assessed, and that appropriate action is taken to mitigate them; and

(b) **ICT support systems** – controls that provide reasonable assurance that ICT security mechanisms support the needs of UNSOA.

10. OIOS conducted the audit from 5 May to 13 June 2014. The audit covered the period from 1 November 2013 to 30 April 2014.

11. OIOS conducted an activity-level risk assessment to identify and assess specific risk exposures, and to confirm the relevance of the selected key controls in mitigating associated risks. Through review of design and implementation of processes, procedures, and configurations of systems, interviews with staff, and testing of UNSOA network and ICT infrastructure, OIOS assessed the existence and adequacy of internal controls and conducted necessary tests to assess their effectiveness. In particular, OIOS assessed the internal controls related to ICT security policies and procedures, risk assessments, network security, access controls, physical and data security, disaster recovery, and system monitoring.

III. AUDIT RESULTS

12. The UNSOA governance, risk management and control processes examined were assessed as **partially satisfactory**[1] in providing reasonable assurance regarding the **effective management of ICT security in UNSOA.** OIOS made five important recommendations to address issues identified in the audit. UNSOA had adopted some good practices for ICT security in the areas of system monitoring, protection of data, media and software, and hardware and communication links. However, some control weaknesses were identified with regard to: (i) incomplete ICT security policies and procedures; (ii) inadequate ICT security risk assessments and physical access controls; (iii) lack of a formal change management policy; (iv) inadequate planning for disaster recovery; and (v) incomplete incident and response management.

13. The initial overall rating was based on the assessment of key controls presented in Table 1 below. The final overall rating is **partially satisfactory** as implementation of four important recommendations remains in progress.

Table 1: Assessment of key controls

Business objective	Key controls	Control objectives			
		Efficient and effective operations	**Accurate financial and operational reporting**	**Safeguarding of assets**	**Compliance with mandates, regulations and rules**
Effective management of ICT security in UNSOA	(a) Risk assessment	Partially satisfactory	Partially satisfactory	Partially satisfactory	Partially satisfactory
	(b) ICT support systems	Partially satisfactory	Partially satisfactory	Partially satisfactory	Partially satisfactory
FINAL OVERALL RATING: PARTIALLY SATISFACTORY					

[1] A rating of **"partially satisfactory"** means that important (but not critical or pervasive) deficiencies exist in governance, risk management or control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

A. Risk assessment

<u>Weaknesses in security risk assessments</u>

14. Risk assessment is an essential activity for monitoring, evaluating and managing risks relating to ICT systems. Periodic vulnerability tests of ICT systems should be conducted, and adequate controls implemented, to prevent or reduce the negative impact of the potential exploitation of network vulnerabilities.

15. Although UNSOA had an ICT security and compliance officer and a dedicated ICT security focal point, there were no mechanisms in place for the periodic and systematic conduct of ICT security risk assessments. The absence of regular risk assessments could prevent the timely identification and mitigation of ICT security risks.

16. UNSOA had a plan to conduct network vulnerability tests on a regular basis and included this task in its disaster recovery plan. However, given that the local area network at the mission level was being reconfigured and that dedicated tools were not yet available, network vulnerability tests were not conducted.

17. OIOS conducted network vulnerability tests of the UNSOA local area network in Nairobi, Mombasa and Mogadishu. Given the confidentiality of these results, the outcome of the tests was shared and discussed directly with the Chief of ICTS and the relevant staff (i.e., ICT Network and Security Officers) of UNSOA for their immediate analysis and mitigation.

18. Lack of periodic ICT vulnerability testing could lead to breaches of security, potential losses of information assets and unavailability of ICT systems and applications.

(1) UNSOA should: (i) conduct periodic and systematic ICT security risk assessments to identify and mitigate potential security vulnerabilities; and (ii) assess the network vulnerabilities and implement adequate measures for their mitigation, including the establishment of procedures for the periodic conduct of ICT vulnerability tests.

19. *UNSOA accepted recommendation 1 and stated that it has: (i) already acquired the vulnerability software to assess network threats, and the firewalls to provide improved security; and (ii) drafted an internal standard operating procedure with a schedule for the conduct of regular ICT vulnerability tests.* Recommendation 1 remains open pending receipt of documented evidence showing the results of periodic and systematic ICT security risk assessments conducted in UNSOA, and that adequate measures have been put in place to mitigate network vulnerabilities.

<u>Incomplete policies and procedures framework</u>

(a) ICT Security

20. Organizations should define information security policies and procedures and assign specific responsibilities for their operation, monitoring, and compliance.

21. UNSOA had some draft security policies (i.e., remote connections, file sharing management, configuration of access control rights, and virtual private network), and implemented several automated controls, including the use of a dedicated tool for patch management. However, additional provisions

were still needed to complete the ICT security management system in accordance with the security framework established by the Secretariat, including:

(i) ICT security plan;

(ii) Processes for enforcing ICT security policies and procedures;

(iii) Definition of roles and responsibilities for ICT security; and

(iv) Periodic ICT security awareness training for the user community.

22. The absence of complete information security policies and procedures could prevent UNSOA from assessing and effectively managing ICT security risks that could potentially lead to loss of information assets.

(b) Access control risks

23. User access to systems and applications should be controlled with procedures and mechanisms to request, grant, suspend, modify and terminate access to systems and related privileges. These procedures should apply to all users, for both standard and emergency cases.

24. UNSOA developed various documents on access controls, based on the ICT access rights and password security policies. Network access was managed using the active directory. There was also a project in progress to restrict access to critical resources and reduce the number of domains and system administrators, as well as assign dedicated access rights to technicians. However, UNSOA did not yet have an access control policy defining the specific roles, responsibilities and procedures to create, monitor, update and terminate user accounts.

25. The absence of adequate mechanisms for managing user access to UNSOA systems increased the risk of unauthorized access.

(c) Incomplete change and release management

26. A change management policy should include control mechanisms to ensure that changes to the ICT infrastructure and applications, including emergency maintenance and patches, are adequately reviewed, approved, monitored and reported. Changes should be logged, assessed and authorized prior to their implementation.

27. Although UNSOA managed changes to its ICT infrastructure through the use of ad-hoc processes and templates, the ICT change and release management policy was still in draft form and not enforced.

28. The absence of a formally approved and enforceable change management policy may have a negative impact on the continuity and security of ICT operations, and potentially lead to loss of data.

(d) Incomplete incident and response management

29. A consistent and effective approach to the management of information security incidents, including communication of security events and weaknesses, should be in place through a documented incident and response management policy.

30. The incident and response management procedure developed by UNSOA was in draft form and did not contain clear information about the authorship of the document. There was no evidence of tools and documented reports demonstrating that the procedure had been implemented as expected.

31. Information security incidents may not be managed consistently and appropriately in the absence of a documented incident management policy.

(2) UNSOA should complete its ICT policies and procedures framework with: (i) an ICT security plan; (ii) processes for enforcing ICT security policies and procedures; (iii) definition of roles and responsibilities for ICT security; (iv) periodic ICT security awareness training of the user community; (v) an access control policy defining the roles and responsibilities to create, monitor, update and terminate user accounts; (vi) ICT change and release management procedures; and (vii) an incident management policy.

32. *UNSOA accepted recommendation 2 and stated that: (i) the current ICT security plan includes processes for enforcing ICT security policies and procedures, with defined roles and responsibilities; (ii) management will ensure that all newcomers receive orientation on basic ICT awareness and training, with posters reminding users about security threats; (iii) the access control policy defining roles and responsibilities is in place; (iv) a change and incident management policy is being formalized and a database is in place; and (v) management will review the current security plan in accordance with existing configuration of the network and infrastructure.* Recommendation 2 remains open pending receipt of the documented evidence of the ICT security plan, security policies and procedures, definition of roles and responsibilities, security awareness training, access control policy, ICT change and release management procedures, and incident management policy.

B. ICT support systems

Network security control weaknesses

33. Networks should be managed and controlled to protect information stored and processed by ICT systems and applications.

34. UNSOA had dedicated network and security administrators, and implemented multiple layers of security controls, including the use of firewall and virtual private networks. Procedures and guidelines for administering critical network components (i.e., firewalls, routers, switches, virtual private network and the demilitarized network zone) were in place. However, UNSOA was still in the process of reviewing and renaming the administrator accounts for network management from their default settings.

35. Default administrator accounts for network management may expose UNSOA network to the risk of unauthorized access.

(3) UNSOA should expedite the review and renaming of the administrator accounts.

36. *UNSOA accepted recommendation 3 and stated that the administrator accounts have been renamed and passwords changed.* Recommendation 3 remains open pending receipt of evidence demonstrating the completion of the review and renaming of the administrators' accounts.

Inadequate planning for disaster recovery

37. A business continuity plan should define how an organization will continue operating in response to adverse events. The plan should include instructions defining the actions required by all parties responsible to ensure the continuation of operations under adverse conditions. An ICT disaster recovery plan should be developed in conjunction with the business continuity plan, and provide recovery strategies to meet the objectives of the plan.

38. UNSOA had developed a disaster recovery plan in April 2014. OIOS review of the plan identified some control areas requiring additional actions, such as approval and versioning of the plan, ensuring the completeness of data, performing a risk assessment, and specifying the requirement for post-resumption reviews.

39. The absence of adequate business continuity and disaster recovery arrangements could lead to failure in the timely recovery of ICT systems and applications, and unavailability of critical communications systems.

(4) UNSOA should ensure that its disaster recovery plan is formally finalized and complete with relevant details, including the requirement for a risk assessment and post-resumption reviews.

40. *UNSOA accepted recommendation 4 and stated the disaster recovery plan has been finalized and tested. The second disaster recovery exercise is scheduled to take place by the end of December 2014.* Recommendation 4 remains open pending receipt of the approved and updated disaster recovery plan.

Physical security weaknesses

41. Unauthorized physical access, damage and interference to the organization's information and communications processing facilities need to be prevented by implementing adequate physical and environmental security controls.

42. OIOS conducted physical inspections of the UNSOA ICT installations in Nairobi, Mombasa and Mogadishu. Installations were protected with adequate security measures for access control, fire extinguishing, environmental controls, and power generators. However, in Mogadishu, the perimeter wall surrounding the primary data centre was not adequate and given the proximity of the installation to outside areas, it exposed the Mission to increased risks of unauthorized access and potential downtime.

43. Weakness in controls around physical and environmental security may expose the Mission to the risk of unauthorized access to its ICT facilities.

(5) UNSOA should strengthen the perimeter protection surrounding the primary data centre in Mogadishu.

44. *UNSOA accepted recommendation 5 and stated that the reinforcement of the perimeter protection of the primary data centre in Mogadishu has been completed.* Recommendation 5 is closed based on the photographic evidence of the newly constructed perimeter provided by UNSOA.

IV. ACKNOWLEDGEMENT

45. OIOS wishes to express its appreciation to the Management and staff of UNSOA for the assistance and cooperation extended to the auditors during this assignment.

(*Signed*) David Kanja
Assistant Secretary-General for Internal Oversight Services

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of information and communications technology security in the United Nations Support Office for the African Union Mission in Somalia

Recom. no.	Recommendation	Critical[2]/ Important[3]	C/ O[4]	Actions needed to close recommendation	Implementation date[5]
1	UNSOA should: (i) conduct periodic and systematic ICT security risk assessments to identify and mitigate potential security vulnerabilities; and (ii) assess the network vulnerabilities and implement adequate measures for their mitigation, including the establishment of procedures for the periodic conduct of ICT vulnerability tests.	Important	O	Receipt of documented evidence demonstrating the results of periodic and systematic ICT security risk assessments conducted in UNSOA, and that adequate measures have been put place to mitigate network vulnerabilities.	31 December 2014
2	UNSOA should complete its ICT security policies and procedures with: (i) an ICT security plan; (ii) processes for enforcing ICT security policies and procedures; (iii) definition of roles and responsibilities for ICT security; and (iv) periodic ICT security awareness training of the user community; (v) an access control policy defining the roles and responsibilities to create, monitor, update and terminate user accounts; (vi) ICT change and release management procedures; and (vii) an incident management policy.	Important	O	Receipt of documented ICT security plan; security policies and procedures; definition of roles and responsibilities; awareness training; access control policy; ICT change and release management procedures; and incident management.	31 December 2014
3	UNSOA should expedite the completion of the review and renaming of the administrator accounts.	Important	O	Receipt of evidence demonstrating the completion of the review and renaming of the administrators' accounts.	31 December 2014
4	UNSOA should ensure that its disaster recovery plan is formally finalized and complete with relevant details, including the requirement for a risk assessment and post-resumption reviews.	Important	O	Receipt of the approved and updated disaster recovery plan.	31 December 2014

[2] Critical recommendations address significant and/or pervasive deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance cannot be provided regarding the achievement of control and/or business objectives under review.
[3] Important recommendations address important deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.
[4] C = closed, O = open
[5] Date provided by UNSOA in response to recommendations.

STATUS OF AUDIT RECOMMENDATIONS

Audit of information and communications technology security in the United Nations Support Office for the African Union Mission in Somalia

Recom. no.	Recommendation	Critical[2]/ Important[3]	C/ O[4]	Actions needed to close recommendation	Implementation date[5]
5	UNSOA should strengthen the perimeter protection surrounding the primary data centre in Mogadishu.	Important	C	Action completed.	Implemented

APPENDIX I

Management Response

United Nations Support Office for AMISOM (UNSOA)

Interoffice Memorandum

To: Mr. Gurpur Kumar, Deputy Director
Peacekeeping Audit Service
Internal Audit Division,
OIOS

Date: 24 November 2014

From: Wolfgang Weiszegger
Acting Director

Ref: UNSOA/1114/M.014

Subject: Assignment No. AT2014/638/02 – Draft report on an audit of information and communications technology security in UNSOA

1. Further to your memorandum of 10 October 2014 (Ref: IAD: 14-00682) on the above subject, please find attached the UNSOA response.

2. Management would like to address the data presented in the background portion of the document (Paragraphs 3, 4 and 5), which should correctly read as below:

a) Para 3

UNSOA provides logistical support to the African Union Mission in Somalia (AMISOM) whose staff are mostly located in Mogadishu, the United Nations Assistance Mission in Somalia (UNSOM), the Office of Special Envoy of the Secretary General for the Great lakes Region (O/SESG-GLR) in Nairobi; and the Somalia-Eritrea Monitoring Group (SEMG), also based in Nairobi. UNSOA also provides Umoja support and performs transactions for UNSOM, O/SESG-GL and SEMG.

b) Para 4

The Budget of UNSOA for the 2013/2014 period was US $433.9 million with 241 international and 160 national staff, to support the increased full authorized strength of AMISOM troops of 22,126, 260 individual police officers, 280 formed police personnel, 70 AMISOM civilian staff as well as up to 10,900 Somalia National Army troops, pursuant to UN Security Council Resolution 2124 (2014).

c) Para 5

The Information and Communications Technology Section (ICTS) of UNSOA supports and maintains 26 VSAT systems, 19 microwave links, 4 containerized modular data centres, 18 communication containers, 3 mobile deployable telecommunications systems (MDTS), 28 physical servers, 250 virtual servers, 237 desktop computers and thin clients, 511 laptop computers, 62 printers, 11 Wide Area Networks and 9 Local Area Networks in nine locations to support United Nations and AMISOM personnel. In addition, ICTS supports the ICT infrastructure in Mogadishu to enable UNSOA to remotely support AMISOM in-theatre operations, and maintains 1,070 e-mail accounts of UNSOA, UNSOM, AMISOM, SESG-GL, and SEMG personnel.

3. Management further observes that the memorandum transmitting the draft audit report was addressed to Mr. Augustine Mahiga, the last Special Representative of the Secretary-General while UNPOS was extant. It should be noted that the mandate of UNPOS was not continued beyond June 2013. The United Nations Assistance Mission in Somalia was established as a new entity in June 2013, with Mr. Nicholas Kay as the inaugural SRSG. It should further be noted that UNSOA was established as an independent office under the direct Management of the USG for Field Support. Consequently, audit reports emanating from IAD/OIOS are addressed to the Director of UNSOA, as was done with the Detailed Audit Results for the subject exercise.

4. Management regrets the delay in response, which is due to the need to ensure that all areas of the observations and recommendations have been exhaustively addressed.

Best regards

cc: Mr. Dionne Maxwell, Audit Focal Point, Umoja Office, DM

Mr. Harjit Dhindsa, Deputy Director, UNSOA
Mr. Robert Kirkwood, Head of Somalia Support, UNSOA
Mr. Jason Mayordomo, Chief of Communications Information Technology Section, UNSOA
Mr. Zachary Ikiara, Chief, Oversight and Coordination Support Unit, DM
Ms. Cynthia Avena-Castillo, Professional Practices Section, Internal Audit Division, OIOS
Ms. Dolapo Kuteyi, Senior Administrative Officer/Audit Focal Point, UNSOA

APPENDIX I

Management Response

Audit of information and communications technology security in the United Nations Support Office for the African Union Mission in Somalia

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	UNSOA should: (i) conduct periodic and systematic ICT security risk assessments to identify and mitigate potential security vulnerabilities; and (ii) assess the network vulnerabilities and implement adequate measures for their mitigation, including the establishment of procedures for the periodic conduct of ICT vulnerability tests.	Important	Yes	CCITS	31/12/2014	Management has already acquired the Nessus Vulnerability software *(See attached Annex 1)* to assess network susceptibilities and also acquired checkpoint firewalls to provide a strong level of gateway security and identity awareness, which has arrived in the Mission on 30 October 2014 and is in the process of being implemented. UNSOA has drafted an internal SOP with a schedule to conduct regular ICT vulnerability tests and related mitigation measures which will be finalized in December 2014.
2	UNSOA should complete its ICT security policies and procedures with: (i) an ICT security plan; (ii) processes for enforcing ICT security policies and procedures; (iii) definition of roles and responsibilities for ICT security; and (iv) periodic ICT security awareness and training of the user community; (v) design and implement an access control policy defining the roles and responsibilities to create, monitor, update and terminate user accounts; (vi) ICT change and release management procedures; and (vii) incident management	Important	Yes	CCITS	31/12/2014	The current UNSOA ICT security includes an ICT security plan, which reflects the processes for enforcing ICT security policies and procedures and the definitions of roles and responsibilities for ICT security. *(see Annex 2)* Management will ensure that all newcomers receive orientation on basic ICT awareness and training. Posters are also being used to remind users on how to deal with security threats. The access control policy defining the roles and responsibilities is also in place. *(See Annex 2A*

[1] Critical recommendations address significant and/or pervasive deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance cannot be provided regarding the achievement of control and/or business objectives under review.

[2] Important recommendations address important deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

Management Response

Audit of information and communications technology security in the United Nations Support Office for the African Union Mission in Somalia

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	policy.					*and Annex 3)* UNSOA management has been practicing change and incident management within the applications using a change and incident management database. Management is in the process of formalizing change and incident management policies. Management will review the current security plan in accordance with existing set-up and configuration of the network and system infrastructure.
3	UNSOA should expedite the completion of the review and renaming of the administrator accounts.	Important	Yes	CCITS	Implemented	UNSOA has accomplished the renaming of administrator accounts. Passwords are changed and securely managed *(Annex 3)* Management requests the closure of this recommendation.
4	UNSOA should ensure that its disaster recovery plan is formally finalized and complete with relevant details, including the requirement for a risk assessment and post-resumption reviews.	Important	Yes	CCITS	31/12/2014	Management has tested and finalized the disaster recovery plan, *(Annex 4.)* The second disaster recovery exercise is scheduled to take place by end December 2014.
5	UNSOA should strengthen the perimeter protection surrounding the installation of the primary data centre in Mogadishu.	Important	Yes	CCITS	Implemented	The reinforcement of the perimeter protection of the primary data centre in Mogadishu has been completed *(Annex 5)* Management requests closure of this recommendation.