INTERNAL AUDIT DIVISION

AUDIT REPORT

ICT governance and security management in UNOCI

Additional controls are required to ensure the effectiveness and security of ICT operations

16 March 2011
Assignment No. AT2010/640/01

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.Y.J.Choi, DATE: 16 March 2011
A: Special Representative of the Secretary-General,
United Nations Operation in Côte d'Ivoire

REFERENCE: IAD: 11- 00286

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

SUBJECT: **Assignment No. AT2010/640 /01 - Audit of ICT governance and security management in**
OBJET: **UNOCI**

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

2. Based on your comments, we are pleased to inform you that we will close recommendations 6, 9, 10, 11 and 15 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. Your response indicated that you did not accept recommendation 3a. In OIOS' opinion however, this recommendation seeks to address significant risk areas. We are therefore reiterating it 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 13, and 16), in its annual report to the General Assembly and semi-annual report to the Secretary-General.

cc: Mr. Choi Soon-hong, Assitant Secretary-General, Chief Information Technology Officer
Mr. Gianni Deligia, Chief of Mission Support, UNOCI
Ms. Elizabeth George, Chief Integrated Support Services, UNOCI
Mr Rudy Sanchez, Director Information Technology Division, DFS
Mr. Vijayaratnam Rajaratnam, Chief Communications and Information Technology Section, UNOCI
Mr. Swatantra Goolsarran, Executive Secretary, UN Board of Auditors
Ms. Susanne Frueh, Executive Secretary, Joint Inspection Unit
Mr. Jonathan Childerley, Chief, Oversight Support Unit, Department of Management
Mr. Byung-Kun Min, Special Assistant to the USG, OIOS
Mr. Seth Adza, Chief Audit Response Team, DFS
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

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: kumarg@un.org

EXECUTIVE SUMMARY

Audit of ICT governance and security management in UNOCI

OIOS conducted an audit of information and communications technology (ICT) governance and security management in the United Nations Operation in Côte d'Ivoire (UNOCI). The overall objective of the audit was to assess the adequacy and effectiveness of internal controls over ICT operations and information security management, and to determine compliance with applicable United Nations regulations, rules, policies and procedures. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

UNOCI had several controls for supporting ICT operations and security management, which facilitated the governance of ICT resources and the development of the infrastructure in the Mission. In particular, OIOS noted good controls in the following areas:

(i) The user community positively assessed the support provided by the Communications and Information Technology Section (CITS);

(ii) A disaster recovery plan test and validation exercise was completed in November 2009;

(iii) A service level agreement (SLA) existed between CITS and the Public Information Unit (PIU). In OIOS' opinion similar agreements should be extended to other critical services within the mission (i.e., Geographical Information Section); and

(iv) Procedures had been formalized and implemented for the checking in and out (CICO) process and extended to include local contractors.

However, UNOCI needed to implement additional controls to further develop processes and document procedures for reinforcing the ICT governance structure, service delivery, and the security of ICT operations. The following opportunities for improvement were noted:

(i) Development of a local ICT strategy and the establishment of an ICT governance framework and an ICT steering committee;

(ii) Documentation of standard operating procedures aligned with those established by the Office of Information and Communications Technology (OICT) and the implementation of the United Nations standard project management methodology and risk management framework;

(iii) Definition of the information architecture of the Mission and the documentation of procedures and criteria for the classification of data and cataloging ICT services;

(iv) Generation of reports and statistics for monitoring ICT performance and capacity management and establishing problem reporting procedures between the sectors and UNOCI headquarters; and

(v) Implementation of additional controls to strengthen the information security function in the areas of training, independent assessments, physical security, communications, incident management, vulnerability testing, disaster recovery and implementation of procedures for the secure removal of data from storage media and devices.

.

TABLE OF CONTENTS

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 Operation in Côte d'Ivoire (UNOCI). The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

2. UNOCI was established by Security Council resolution 1528 of 27 February 2004 and further developed by resolution 1609 of 24 June 2005. The most recent extension of the mandate was approved by the Security Council in its resolution 1962 (2010), by which the mandate was extended until 30 June 2011. The mission's main objective is to facilitate the implementation of the 2003 peace agreement by the Ivorian parties.

3. The Mission is currently organized in two sectors, with its headquarters located in the capital, Abidjan. The sector west headquarters is Daloa and sector east Headquarters is Bouake.

4. The Mission's strength as of 30 August 2010 is 8,542 total uniformed personnel, including 7,186 troops and 189 military observers; 1,167 police; supported by 393 international civilian personnel, 759 local staff, 274 United Nations Volunteers.

5. The Communication and Information Technology Section (CITS) provides ICT services to the Mission. It is staffed by 49 international, 59 national and 5 general temporary assistance (GTA) staff.. Four posts were vacant.

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

II. AUDIT OBJECTIVES

7. The main objectives of the audit were to assess the adequacy and effectiveness of internal controls over ICT governance and security management and to determine compliance with applicable United Nations regulations, rules, policies and procedures. In particular, the audit assessed whether the following controls were in place:

<u>ICT governance</u>

(i) An organizational structure for governing, managing, and protecting ICT resources and data;

(ii) Mechanisms for identifying and managing ICT risks;

(iii) ICT roles, responsibilities, and reporting lines;

(iv) Processes for ICT strategic planning, monitoring, reporting, and continuous improvement;

(v) Mission specific ICT policies and standard operating procedures;

(vi) Procedures for managing ICT assets; and

(vii) A standard management methodology for ICT projects and initiatives.

ICT security management

(i) ICT security policies and procedures;

(ii) Security risk assessments and vulnerability tests;

(iii) Security awareness and training initiatives; and

(iv) Standard terms of reference and procedures for: configuration management; access control; contingency planning; incident management; systems' control; protection of software, hardware and communication links; data and media protection; physical security; personnel security; malicious software; and monitoring.

III. AUDIT SCOPE AND METHODOLOGY

8. The audit covered the period 1 January 2009 to September 2010 and focused on testing the effectiveness of the controls in accordance with the United Nations regulations and rules and generally accepted professional standards (i.e. Control Objective for Information and related Technology and the international standard for information security management ISO 27001).

9. The audit methodology included the assessment and testing of internal controls, interviews with personnel, review of relevant documentation, and physical observation of and site visits to ICT installations.

IV. AUDIT RESULTS

A. Strategic planning and governance

10. A strategy should give direction and establish priorities for the investments and management of ICT resources. The strategy should be complemented by an ICT governance framework defining the distribution of the decision-making roles and responsibilities among different offices in the organization, and establishing procedures for implementing and monitoring the strategic decisions.

11. Although UNOCI had an established ICT Review Committee responsible for reviewing and approving ICT projects, this Committee had not met in the last three years while, during the same time period, CITS developed and implemented over sixty-one projects. The following additional control weaknesses were noted:

(i) UNOCI did not document a local ICT strategy defining how the provision of ICT services could contribute and support the missions mandate and objectives;

(ii) There were no formal procedures for approving and reporting ICT performance (quantitative and qualitative) in a systematic manner;

(iii) The majority of CITS units were operating without standard operating procedures (SOPs); and

(iv) There was a fragmented approach to ICT service delivery within the Mission. ICT services provided by the Mission Headquarters were defined and had adequate resources for meeting the needs of HQ users, but the ICT services and resources available in the Sectors were not adequate.

12. These conditions exposed UNOCI to the risk of: (i) lack of accountability and direction; (ii) inability to meet ICT needs of the organization; and (iii) ICT not being given sufficient strategic importance.

Recommendations 1

(1) The UNOCI Division of Mission Support should: (a) Document a local ICT strategy defining how ICT service provisions will contribute to and support the Mission's goals and operational needs; (b) Design and implement an ICT governance framework and re-activate the ICT Steering Committee, reviewing the terms of reference of the Committee to include responsibilities for providing direction, control and approval of ICT investments; and (c) Document standard operating procedures for approving and reporting ICT performance in alignment with those established at UNHQ.

13. *UNOCI accepted recommendation 1 and stated that its goal was to implement the Information Technology Infrastructure Library (ITIL) framework at Maturity Level 1.5 across all module and that it will reactivate the steering committee through the office of the Chief of Mission Support. It further stated that it will establish key performance indicators (KPIs) for all CITS units and gather daily, weekly and monthly statistics.* Based on the actions planned by UNOCI, recommendation 1 is closed. Recommendation 1 remains open pending receipt of the documented ICT strategy, governance framework and standard operating procedures for reporting and approving ICT performance.

Information architecture

14. Information architecture is a conceptual framework that defines the flow of information and the basic structure, content, and relationships of the

applications and systems employed by an organization to process the data needed in support of its activities.

15. UNOCI had not defined its information architecture and how the ICT infrastructure and operations will be structured to enable the achievement of its goals and objectives. In the absence of defined and complete information architecture, UNOCI would not be able to achieve a consistent approach to information systems management, avoid duplications, and maximize the use of applications.

Recommendation 2

(2) The UNOCI Communication and Information Technology Section should document its information architecture for all applications in use in the Mission, complete with systems, ownership, substantive programmes supported, and their relationship with the ICT strategic plan.

16. *UNOCI accepted recommendation 2 and stated that it will create a service catalog as part of the ITIL framework.* Recommendation 2 remains open pending documentation of the information architecture.

Project management

17. A standard project management methodology provides a structured approach for documenting and communicating to stakeholders the critical elements of a project. The Information and Communications Technology Division (ICTD) in DFS indicated in its "vision paper" for the activities 2009-2010 that the methodology "Project in a controlled environment version 2" (PRINCE2) was the standard project management methodology of the department. This methodology had been formally implemented in UNOCI.

18. However, OIOS noted that in the implementation of the project management methodology, CITS:

(i) Had not established adequate segregation of responsibilities between project management and application development, and the same staff was responsible for both activities;

(ii) Internally developed 61 applications which were not built on the basis of a standard development lifecycle and structured project management methodologies. OIOS acknowledges that some of these applications (i.e. telephone billing systems and electronic movement of personnel) were developed before DFS adopted PRINCE2 and were urgently needed for supporting mission processes;

(iii) Did not assess whether the applications locally developed will be replaced or interfaced with the new enterprise-wide information systems of the United Nations Secretariat such as Enterprise Resource Planning

(ERP/UMOJA), Customer Relationship Management (CRM-i-Need) and Enterprise Content Management (ECM); and

(iv) Although, in accordance with the ICT roadmap for field Missions issued by DFS/UNHQ in 2008, requests for the development of new applications had to be reviewed/approved by the ICT Review Committee (ICTRC) on the basis of documented business cases, the applications developed in UNOCI did not include minimum requirements related to: (i) Functional needs; (ii) Disaster recovery and business continuity; (iii) Security; iv) Integration and reporting; and (v) Verification of existing working practices and applications developed in other Missions.

19. The current status of controls in place may expose UNOCI to the risk of: (i) unrealistic expectations; (ii) lack of consistency in managing projects and reporting on their performance; (iii) inability to compare and benchmark; and (iv) duplication and inefficiencies.

Recommendations 3

(3) The UNOCI Communication and Information Technology Section should: (a) formally implement control mechanisms in accordance with the standard United Nations project management methodology PRINCE2 for preparing, reviewing, approving, and managing ICT projects and initiatives; and (b) Undertake a comprehensive review of all locally developed applications to determine their level of integration with the new enterprise applications ERP/UMOJA, CRM-i-Need and ECM.

20. *UNOCI did not accept recommendation 3a, stating that high level project management is difficult if there is no effective control and that ITIL Configuration Management, Release and Change Management need to be established first.* OIOS is unable to accept this response because OICT has established the PRINCE2 as the standard project management methodology for ICT projects in the United Nations Secretariat and developed a handbook for its adoption. UNOCI should refer to the PRINCE2 based project management handbook developed by OICT, which also provides the tools and templates for developing ICT projects. Recommendation 3a remains open pending the implementation of control mechanisms in accordance with the standard project management methodology PRINCE2 for preparing, reviewing, approving, and managing ICT projects and initiatives.

21. *UNOCI accepted recommendation 3b stating that it will: (i) Undertake an analysis of integration with UN based enterprise applications; (ii) Remove unused applications; and (iii) Develop new Standard Operating Procedures (SOP) on UNOCI applications and their support by CITS.* Recommendation 3b remains open pending receipt of evidence demonstrating the results of the analysis of integration with UN based enterprise applications and the documented standard operating procedures.

Risk management

22. Periodic risk assessments should be conducted to identify threats that could negatively impact ICT operations and assets. Documentation shall demonstrate the relationship between the risks identified and the mitigating measures implemented to address them, and their corresponding treatment plans.

23. CITS did not establish an ICT risk management framework to identify risks and corresponding mitigating controls. However, OIOS was informed that staff had been trained on risk management and a tool is currently available in support of this function.

Recommendation 4

(4) The UNOCI Division of Mission Support should establish a risk management framework and implement procedures to address ICT risks identified and implement corresponding mitigating controls.

24. *UNOCI accepted recommendation 4 and stated that risk analysis will be added to the disaster recovery and business continuity (DRBC) document.* Recommendation 4 remains open pending the establishment of a risk management framework and the implementation of procedures to address ICT risks.

ICT operations, planning and control

25. The use of ICT resources should be regularly monitored and projections made to determine future capacity requirements, ensuring a constant and reliable level of performance measured against pre-defined quantitative and qualitative metrics.

26. The system of controls in place in UNOCI lacked the following procedures:

(a) Standard operating procedures (SOPs) for the configuration, integration and maintenance of hardware, infrastructure and software to protect ICT resources and ensure their availability and integrity, in accordance with pre-defined metrics;

(b) An ICT operational work plan for ensuring management and control of ICT operations across the mission;

(c) A disposal policy on ICT equipment with defined arrangements for the secure disposal of removable media. Equipment containing storage media (hard-drives and other removable media) were not always sanitized to ensure that any sensitive data and licensed software had been removed or securely overwritten prior to transfer of ownership or disposal; and

(d) Adequate procedures to identify and timely respond to the needs of ICT staff in the field sectors. OIOS was informed that in the South West HQ sector, only three vehicles were available to CITS to cover 13 sites. Some of the sites were approximately 400 km. apart.

27. Undefined SOPs and the absence of quantitative and qualitative metrics for monitoring and measuring ICT operations may prevent CITS from detecting and addressing in a timely manner problems with the quality and quantity of services provided to the Mission.

Recommendations 5 and 6

The UNOCI Communication and Information Technology Section should:

(5) Document and implement: (a) Standard procedures and guidelines for the configuration, integration and maintenance of hardware and infrastructure software; (b) An ICT operational plan for initiatives, resource requirements, and quantified estimated benefits; and (c) Procedures for the secure removal of data from storage media and for sanitizing removable devices prior to their transfer or disposal; and

(6) In collaboration with the Transport Section, should review its allocation of vehicles to the Sector HQ and ensure that there are adequate vehicles to attend to problems in remote locations.

28. *UNOCI accepted recommendation 5 stating that configuration management will be part of the implementation of the ITIL framework and that that a guideline will be created based on existing operational procedures.* Recommendation 5 remains open pending documentation of: (a) standard procedures and guidelines for configuration, integration and maintenance of hardware and infrastructure software; (b) An ICT operational plan; and (c) Documentation of procedures for the secure removal of data from storage media.

29. *UNOCI accepted recommendation 6 and stated that the Mission Vehicle Establishment Committee (VEC) will determine distribution of vehicles.* Based on the actions planned by UNOCI, recommendation 6 is closed. OIOS will confirm the implementation of these actions during a follow-up review.

Data classification

30. ST/SGB/2007/6 (Information sensitivity, classification and handling) requires the classification of data for defining ownership, security levels (confidentiality, integrity and availability), retention schedules, and destruction requirements.

31. UNOCI did not have documented procedures to ensure that common standards were applied within the Mission for the storage of records and archives, and to ensure compliance with ST/SGB/2007/6.

32. The current condition of the controls in place for managing ICT assets in UNOCI exposed the Mission to risks associated with inadequate protection of sensitive data and loss of information assets.

Recommendation 7

(7) The UNOCI Division of Mission Support should document procedures ensuring: (a) The application of standards for data classification and archiving; and (b) The integrity and consistency of data stored in electronic form.

33. *UNOCI accepted recommendation 7 stating that as part of a Mission wide business continuity implementation: i) All sections will be tasked to identify and classify their critical data; and ii) CITS will issue a policy document in this regard.* Recommendation 7 remains open pending documentation of procedures for data classification and archiving, and integrity and consistency of data stored in electronic form.

B. Acquisition and implementation

Management of service level agreements

34. ICT operations should be planned and controlled on the basis of terms of reference defining the level of service expected by the clients. These terms of reference should:

(i) Define service requirements, delivery agreements, and guides;

(ii) Define performance indicators and monitoring requirements; and

(iii) Complement the standard service catalogue with details about the organizational structure designed by the service provider (ICTS), with roles, tasks and responsibilities.

35. A service level agreement (SLA) existed between CITS and the Public Information Unit (PIU). In OIOS' opinion similar agreements should be extended to other critical services within the mission (i.e., Geographical Information Section). Furthermore, CITS did not document a catalogue of services with requirements, definitions, roles and responsibilities together with quantitative and qualitative metrics on: a) availability; b) reliability; c) performance and d) capacity.

36. CITS did not use automated tools for service desk management and did not generate any reports on help desk activity (e.g. tickets issued and closed, types of service calls received, systemic problems, root-causes analysis, etc.) However, OIOS noted that at the time of the audit CITS was testing an in-house

developed application for the administration of the help desk. In addition, criteria, standards and performance indicators for measuring service delivery were not documented.

Recommendations 8

(8) The UNOCI Communication and Information Technology Section should:

(a) Develop ICT service processes and document service procedures in line with best practice for service delivery (i.e. Information Technology Infrastructure Library). These procedures should include change management, incident management, configuration management, release management, testing of changes, and risk assessments; and

(b) Document the catalogue of services it provides, together with the criteria, standards and performance indicators for service delivery; and

37. *UNOCI accepted recommendation 8 stating that the creation of procedures and the service catalogue will be part of the implementation of the ITIL Framework.* Recommendation 8 remains open pending development of service processes and procedures in line with best practice for service delivery (ITIL).

Asset management

38. The protection of assets should be supported with controls that include: (i) inventory; (ii) definition of their ownership; (iii) acceptable use policies; (iv) classification; and (v) labeling.

39. CITS had a surge in obsolete equipment that had reached the end of their economic useful life. While OIOS observed several equipment awaiting write offs, there was no evidence of a plan in place to manage the write-off of this equipment.

40. In 2008, OIOS conducted an audit of the management of public information programmes in UNOCI (AP2008/640/06) and observed the underutilization of infrastructure equipment. A physical verification of ICT assets at the CITS/AMU (Asset Management Unit) warehouse identified that many of these infrastructure equipment remained in the warehouse and had still not been deployed. These could become obsolete before their utilization.

41. There was a high stock of expendable items such as FAX cartridges in the CITS/AMU warehouse. CITS indicated some issues with delays in the mission's procurement process and the length of time taken to receive critical ICT supplies for the Mission. Faced with the impending elections in Côte d'Ivoire, critical equipment were needed, such as VHF radios were lacking

replacement batteries and long-range HF antenna for the vehicles allocated to the Military staff deployed in the Sector.

42. The inadequacy of controls in place for asset management could expose the Mission to risks related to the inefficient use of resources and financial losses.

Recommendations 9

> **(9) The UNOCI Communication and Information Technology Section, in collaboration with the Department of Field Support, should develop a strategy and criteria for the deployment of equipment to units (including Military staff) on the basis of established and documented requirements, and put in place measures to mitigate the problems with regard to obsolescence and the high stock of expendable items.**

43. *UNOCI accepted recommendation 9 and stated that some analysis already existed on deployment of equipment. It also stated that an Asset Management Unit stock review is underway and fore-casting on expendables will be improved.* Based on the actions being undertaken by UNOCI, recommendation 9 has been closed. OIOS will confirm the implementation of these actions during a follow-up review.

Performance and capacity management

44. The use of ICT resources should be monitored, and projections made of future capacity requirements to ensure the required system performance.

45. CITS had deployed an application ("Solar Wind") for performance and capacity management that supported the following processes: (a) Gathering of data; (b) Monitoring of the performance and capacity of requirements on current usage and the determination of future capacity requirements for the ICT infrastructure; and (c) Planning. However, CITS did not generate reports and statistics on network performance to address: (a) infrastructure resilience; (b) contingency; (c) workloads; (d) storage plans; (e) resource allocation; (f) report delivered service availability; and g) performance and capacity forecasting at regular intervals to identify:

(i) Options for the minimization of risk related to service disruption due to inefficient capacity or performance degradation;

(ii) Excess capacity for possible deployment; and

(iii) Workload trends for future planning.

46. These conditions could cause unexpected incidents due to lack of capacity, system unavailability due to inadequate proactive resource capacity,

and failure to meet organizational requirements due to outdated performance and capacity plans.

Recommendation 10

(10) The UNOCI Communication and Information Technology Section should extract data from the application "Solar Wind" and generate reports and statistics on network performance to address: (a) infrastructure resilience; (b) contingency; (c) workloads; (d) storage plans; (e) resource allocation; (f) to report delivered service availability; and (g) performance and capacity forecasting.

47. *UNOCI accepted recommendation 10 and stated that the "Solar Wind" application has just undergone a major upgrade and will be moved to a new server. CITS is still learning its new capabilities. Reports will be created when staff is sufficiently confident of the accuracy of the collected data.* Based on the actions being undertaken by UNOCI, recommendation 10 has been closed. OIOS will confirm the implementation of these actions during a follow-up review.

Communication links with field sectors

48. Concerns had been raised by the Chief of Military Staff regarding restricted ability to communicate with the sectors and remote sites. Faced with the impending elections, there were several areas of high security risks, which made communication a high priority. Representatives of Military staff indicated that in light of the upcoming elections, there was a need for new antennas and communications devices in the Sectors.

49. OIOS visited the south west sector headquarters and made the following observations concerning CITS' preparedness for the elections in this sector:

(i) Inadequate preparation and lack of planning by CITS Coordination Unit in the sector;

(ii) Inadequate collaboration between CITS in Abidjan and the Sector headquarters for ensuring adequate communication and equipment to facilitate the mission's election mandate and the possible evacuation of mission staff and critical data from the sector HQ and remote sites;

(iii) Low bandwidth availability (256 kb satellite communication links with no redundancies when the satellite links are down), restricting users' ability to access critical applications and network drives;

(iv) Communication radios that did not work at night; and

(v) Users' complaints about the inability of using HF radios, which are critical for long distance communication caused by:

(a) Inadequate training of users on how to operate the radios;

(b) Misuse and abuse of devices;

(c) Design flaw with the HF radio antenna (ATU), which allows water to trickle into the electrical circuit and causes failure of the device; and

(d) Lack of replacement batteries for VHF radios.

Recommendations 11

(11) The UNOCI Communication and Information Technology Section should as a matter of priority, put in place action plans to mitigate the risks faced by the Sectors regarding: (a) low bandwidth; (b) lack of redundancy for the satellite links from the remote sites; (c) design flaws regarding the HF antennas; and (d) replacement of batteries for the VHF radios; and (e) training of critical users in handling the radios.

50. *UNOCI accepted recommendation 11 and stated that issues are being dealt with. It also stated that the current crisis means that CITS needs to readjust its standard goals.* Based on the actions being undertaken by UNOCI, recommendation 11 has been closed. OIOS will confirm the implementation of these actions during a follow-up review.

C. Information security management

Security policy and organization

51. Information security policy and procedures should set clear terms of reference for protecting data and processing systems in line with the organization's rules, regulations and objectives. In addition, information security roles should be assigned across the organization ensuring that dedicated staff follow industrial trends, monitor standards and assessment methods and provide reliable liaison with users. In this area, CITS lacked the following controls:

(i) A formalized ICT security programme e.g reporting data about security events and weaknesses (i.e. virus attacks). This condition limited its ability to: (i) detect and understand the cause of incidents; (ii) obtain timely information for implementing protective measures; and (iii) classify incidents and security breaches based on their causes and attack vectors;

(ii) A dedicated ICT security officer; and

(iii) Independent assessments of information security e.g CITS did not undertake periodic and independent penetration testing, and lacked a

documented and formalized vulnerability management program limiting its capacity for self-assessing the potential vulnerabilities.

52. These control weaknesses expose UNOCI to the risk of improper protection of information assets, loss of confidential information, and unclear understanding of the organization' s IT risk appetite.

Recommendation 12

(12) The UNOCI Communication and Information Technology Section should (a) assign clear responsibilities for ICT security to a dedicated staff member for monitoring ICT security risks and documenting security policies; (b) develop and implement a comprehensive and effective security incident management process: (c) Engage a third party to perform periodic and independent penetration testing; and develop and implement a comprehensive vulnerability management programme.

53. *UNOCI accepted recommendation 12 and stated that CITS is following existing policies dictated by HQ that staff levels do not allow for a 'Security Specialist' and that it will request a post in the budget and funds to create or even assist effectively in vulnerability assessment programme.* Recommendation 12 remains open pending the implementation of a comprehensive and effective security incident management process including the assignment of ICT security duties to a dedicated officer responsible for monitoring ICT security risks and documenting security policies.

Access control

54. Access to information, applications and information processing facilities should be controlled and monitored on the basis of functional needs and security requirements.

55. Although procedures had been formalized and implemented for the checking in and out (CICO) process and extended to include local contractors, OIOS reviewed the user access rights and observed that there were a number of dormant User IDs assigned to staff members that have departed the Mission and had not been removed from all the 14 Windows Active Directory Domain Controllers. Approximately 22 of the 93 staff that had checked out between 15 September and 15 October 2010 still had active User IDs that had not been disabled or deleted. This condition may lead to unauthorized access to data and potential breach of confidential information.

56. The Telephone and Billing Unit makes use of an in house developed application to manage the telephone bills. The application is a web based SQL (Structured Query Language) application which can be accessed via the Intranet. The Chief Communication Officer had full administrative rights over the application and in his absence it was difficult to resolve issues relating to the use of the database. Minimal administrative rights had been provided to other officers

but they were restricted in the level of support they can provide. OIOS also noted that the access granted to the account "Super Admin" was configured without a password.

Recommendation 13

The UNOCI Communication and Information Technology Section should (a) perform a regular review of user access to all critical servers, applications and services to delete User IDs that are no longer required and (b) segregate developer responsibilities from operational responsibilities and ensure that the system administrative rights for the SQL billing application are appropriately allocated. CITS should ensure that it enforces its user naming conventions and the use of passwords for all its administrative accounts.

57. *UNOCI accepted recommendation 13 and stating that the existing "Checking in and checking out" (CICO) procedure will be reviewed and updated regarding CITS staff. It further stated that staffing levels do not allow for role segregation of applications administration staff.* Recommendation 13 remains open pending (a) implementation of a mechanism to perform regular reviews of user access to all critical servers, application and services and (b) the implementation of compensating controls to address the risk of un-segregated responsibilities between development and operations.

Physical and environmental security

58. Controls should be in place to prevent unauthorized physical access, damage, and interference to the organization's premises and information processing facilities.

59. UNOCI did not implement adequate physical and environmental controls for some of its locations housing critical ICT equipment and information such as protection against damage, fire and flood. These gaps could result in the loss of confidentiality, integrity and availability of critical UNOCI information and information assets. The table in Annex 2 documents the list of gaps identified.

Recommendation 14

(14) The UNOCI Communication and Information Technology Section should strengthen the current physical security of its premises with the implementation of the necessary controls to address the weaknesses identified.

60. *UNOCI accepted recommendation 14*, which remains open pending strengthening of the current physical security of its premises.

Security of communications

61. Controls should be in place to ensure the correct and secure operation of communications, with clearly defined responsibilities and procedures, including measures for segregation of duties.

62. OIOS noted that the control system implemented by CITS presented the following weaknesses:

(i) A formalized patch management process was not in place, and the current process was ad-hoc. This condition could lead to disruptions in production processing, technology failing to support operations, and violations of license agreements;

(ii) Lack of an offsite location for storing back-up tapes. All backup tapes were stored in the office of the Chief of CITS. This condition could lead to the unavailability of backup data and media in case of disaster, accidental destruction, and inability to locate backup tapes when needed;

(iii) Backup tapes and drives containing sensitive information were not encrypted, potentially increasing the risk of unauthorized access and breach of confidential data; and

(iv) Inadequate malicious code protection (i.e. antivirus). A recent virus outbreak in the Mission's network was introduced by USB drives. This condition could lead to network disruptions, exposure of information and loss of confidential data.

Recommendation 15

(15) The UNOCI Communication and Information Technology Section should ensure that:

(i) Backup tapes are stored offsite and in fire proof safes;

(ii) Operating procedures are properly documented and followed by all staff and managers;

(iii) Adequate protection measures exist for malicious code prevention such as installation of latest revisions of antivirus programmes and up to date antivirus signatures on all Windows systems;

(iv) Sensitive information is encrypted on all storage devices, tapes, hard drives, and removable media;

(v) Sufficient logging is enabled at the network device, operating system, file level, and application layers; and

(vi) A log correlation tool is implemented for incident management purposes.

63. *UNOCI accepted recommendation 15 and stated that it is moving to Backup to Disk (B2D) and the backup procedures will change as well. (i) B2D means less backup tapes (yearly only). These can be kept in the current location. Numbers (ii) and (iii) are done; (iv) Software is to be acquired; (v) There is limitations in space on the servers which does not allow for continuous logging and a solution is being researched (vi) This will be useful once we reach the ITIL Maturity Level of 3 and Incident and Problem Management are properly defined.* Based on the actions being undertaken by UNOCI, recommendation 15 has been closed.

Disaster recovery and planning

64. Procedures should be in place to counteract interruptions from the effects of failures of information systems or disasters and to ensure their timely resumption. Disaster recovery plans should include provisions for regular tests for validating the reliability of the supporting documentation and processes, and also train and prepare personnel using a simulation of a disaster. In addition, the Mission should have adequate procedures in place to ensure the continuity of its critical processes in case of failure of information systems or disasters.

65. Disaster recovery planning and testing was well established in CITS HQ in Abidjan and a disaster recovery plan test and validation exercise was completed in November 2009. However, the same level of preparedness was not achieved in the field sectors, where disaster recovery plans were not documented or tested. This condition exposed UNOCI to risks of loss of data and the inability to resume operations in case of adverse conditions.

Recommendation 16

(16) The UNOCI Communication and Information Technology Section should complete a comprehensive disaster recovery plan and testing procedures covering all sectors and remote sites of UNOCI.

66. *UNOCI accepted recommendation 16,* which remains open pending the completion of a comprehensive disaster recovery plan and testing procedures.

V. ACKNOWLEDGEMENT

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

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 UNOCI Division of Mission Support should: (a) Document a local ICT strategy defining how ICT service provisions will contribute to and support the Mission's goals and operational needs; (b) Design and implement an ICT governance framework and re-activate the ICT Steering Committee, reviewing the terms of reference of the Committee to include responsibilities for providing direction, control and approval of ICT investments; and (c) Document standard operating procedures for approving and reporting ICT performance in alignment with those established at UNHQ.	Governance	Medium	O	Document ICT strategy, governance framework and standard operating procedures for reporting and approving ICT performance.	June 2011/April 2012
2.	The UNOCI Communication and Information Technology Section should document its information architecture for all applications in use in the Mission, complete with systems, ownership, substantive programmes supported, and their relationship with the ICT strategic plan.	Governance	Medium	O	Document the information architecture.	April 2012
3.	The UNOCI Communication and Information Technology Section should: (a) formally implement control mechanisms in accordance with the standard United Nations project management methodology PRINCE2 for preparing, reviewing, approving, and	Governance	Medium	O	Implement control mechanisms for preparing, reviewing, approving, and managing ICT projects and initiatives.	Not provided

Recom. no.	Recommendation	Risk category	Risk rating	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
	managing ICT projects and initiatives; and (b) Undertake a comprehensive review of all locally developed applications to determine their level of integration with the new enterprise applications ERP/UMOJA, CRM-i-Need and ECM.					
4.	The UNOCI Division of Mission Support should establish a risk management framework and implement procedures to address ICT risks identified and implement corresponding mitigating controls.	Governance	Medium	O	Implement procedures to assess ICT risks.	December 2011
5.	The UNOCI Communication and Information Technology Section should document and implement: (a) Standard procedures and guidelines for the configuration, integration and maintenance of hardware and infrastructure software; (b) An ICT operational plan for initiatives, resource requirements, and quantified estimated benefits; and (c) Procedures for the secure removal of data from storage media and for sanitizing removable devices prior to their transfer or disposal	Information Resources	Medium	O	Document (a) standard procedures and guidelines for configuration, integration and maintenance of hardware and infrastructure software; (b) An ICT operational plan; and (c) Documentation of procedures for the secure removal of data from storage media.	December 2011/April 2012
6.	The UNOCI Communication and Information Technology Section, in collaboration with the Transport Section, should review its allocation of vehicles to the Sector HQ and ensure that there are adequate vehicles to attend to problems in remote locations.	Operational	Medium	C		

Recom. no.	Recommendation	Risk category	Risk rating	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
7.	The UNOCI Division of Mission Support should document procedures ensuring: (a) The application of standards for data classification and archiving; and (b) The integrity and consistency of data stored in electronic form.	Information Resources	Medium	O	Document procedures for data classification and archiving, and integrity and consistency of data stored in electronic form.	
8.	The UNOCI Communication and Information Technology Section should: (a) Develop ICT service processes and document service procedures in line with best practice for service delivery (i.e. Information Technology Infrastructure Library). These procedures should include change management, incident management, configuration management, release management, testing of changes, and risk assessments; (b) Document the catalogue of services it provides, together with the criteria, standards and performance indicators for service delivery; and (c) Conduct a satisfaction survey of its user community to measure the effectiveness of service provision.	Information Resources	Medium	O	Develop service processes and procedures in line with best practice for service delivery (ITIL). Including; procedures ensuring: (a) the application of standards for data classification and archiving; and (b) The integrity and consistency of data stored in electronic form. processes and service procedures in for; a) Change management; b) Incident management; c) Configuration management d) Release management; e) Testing of changes; and f) Risk assessments. Document the ICT catalog of services	April 2012
9.	The UNOCI Communication and Information Technology Section, in collaboration with the Department of Field Support, should develop a strategy and criteria for the deployment of equipment to units (including Military staff) on the basis of established and documented requirements, and put in	Information Resources	Medium	C		

Recom. no.	Recommendation	Risk category	Risk rating	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
	place measures to mitigate the problems with regard to obsolescence and the high stock of expendable items.					
10.	The UNOCI Communication and Information Technology Section should extract data from the application "Solar Wind" and generate reports and statistics on network performance to address: (a) infrastructure resilience; (b) contingency; (c) workloads; (d) storage plans; (e) resource allocation; (f) to report delivered service availability; and (g) performance and capacity forecasting.	Information Resources	Medium	C		
11.	The UNOCI Communication and Information Technology Section should as a matter of priority, put in place action plans to mitigate the risks faced by the Sectors regarding: (a) low bandwidth; (b) lack of redundancy for the satellite links from the remote sites; (c) design flaws regarding the HF antennas; and (d) replacement of batteries for the VHF radios; and (e) training of critical users in handling the radios.	Information Resources	High	C		
12.	The UNOCI Communication and Information Technology Section should (a) assign clear responsibilities for ICT security to a dedicated staff member for monitoring ICT security risks and documenting security policies; (b) develop and implement a	Information Resources	Medium	O	Implement a comprehensive and effective security incident management process including the assignment of ICT security duties to a dedicated officer responsible for monitoring ICT security risks and documenting security policies.	FY 12-13

Recom. no.	Recommendation	Risk category	Risk rating	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
	comprehensive and effective security incident management process: (c) Engage a third party to perform periodic and independent penetration testing; and develop and implement a comprehensive vulnerability management programme.					
13.	The UNOCI Communication and Information Technology Section should (a) perform a regular review of user access to all critical servers, applications and services to delete User IDs that are no longer required and (b) segregate developer responsibilities from operational responsibilities and ensure that the system administrative rights for the SQL billing application are appropriately allocated. CITS should ensure that it enforces its user naming conventions and the use of passwords for all its administrative accounts.	Information Resources	High	O	Implement a mechanism to perform regular reviews of user access to all critical servers, application and services and compensating controls to address the risk of un-segregated responsibilities between development and operations	January/December 2011
14.	The UNOCI Communication and Information Technology Section should strengthen the current physical security of its premises with the implementation of the necessary controls to address the weaknesses identified.	Information Resources	Medium	O	Strengthen the current physical security of the premises.	January 2011
15.	The UNOCI Communication and Information Technology Section should ensure that: (i) Backup tapes are stored offsite and	Information Resources	Medium	C		

Recom. no.	Recommendation	Risk category	Risk rating	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
	in fire proof safes; (ii) Operating procedures are properly documented and followed by all staff and managers; (iii) Adequate protection measures exist for malicious code prevention such as installation of latest revisions of antivirus programmes and up to date antivirus signatures on all Windows systems; (iv) Sensitive information is encrypted on all storage devices, tapes, hard drives, and removable media; (v) Sufficient logging is enabled at the network device, operating system, file level, and application layers; and (vi) A log correlation tool is implemented for incident management purposes.					
16.	The UNOCI Communication and Information Technology Section should complete a comprehensive disaster recovery plan and testing procedures covering all sectors and remote sites of UNOCI.	Information Resources	High	O	Complete a comprehensive disaster recovery plan and testing procedures.	Not provided

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

ANNEX 2

Environmental control weaknesses

Location	Gaps
Main Server Room	The 2 side walls of the main server room are made of unsecured glass and the placement of the only camera is not effective for adequate monitoring ; and There are too many cardboard boxes inside the server room, which could make it easy for fire to breakout in the server room due to combustion.
Airport Server Room/Container	• 2 of the 3 servers are sitting on a raised pallet on the floor of the container instead of being placed in a rack ; and • There is no fire extinguisher and security camera.
Log base Server Room/Container	• The fire extinguisher has wheels so there is a tendency for it to be moved away from reach, this could create a problem in the event of a fire.
CITS AMU Warehouse	• The entrance to the "secure" storage room is a wooden door (double doors) ; and • This combined with the glass windows makes the room fairly easy to break into.
American school server room/ container	No fire extinguishers; No camera for monitoring; and No climate control tool to monitor changes in climatic conditions within the container.