



Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

AUDIT REPORT

Information and communications technology governance and security management in UNMIL

**UNMIL generally had good internal controls but
could strengthen them in the areas of ICT service
delivery, security of operations, and governance
of the ICT infrastructure**

23 July 2010

Assignment No. AT2009/626/01

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: Ms. Ellen Margrethe Løj
A: Special Representative of the Secretary-General,
United Nations Mission in Liberia

DATE: 23 July 2010

REFERENCE: IAD: 10-00662

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

Fatoumata

SUBJECT: **Assignment No. AT2009/626/01 – Audit of information and communications technology
governance and security management in UNMIL**

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 4, 22, 24, 26, and 27 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 recommendations 7, 10, 15, and 17. In OIOS' opinion however, these recommendations seek to address significant risk areas. We are therefore reiterating them and requesting that you reconsider your initial response based on the additional information provided in the report.
4. Please note that OIOS will report on the progress made to implement its recommendations, particularly those designated as high risk (i.e., recommendations 1, 2, 8, 14, 19, 21, 25, 30, and 31), in its annual report to the General Assembly and semi-annual report to the Secretary-General.

cc: Mr. Stephen Lieberman, Chief of Mission Support, UNMIL
Mr. Emmanuel Lemonier, Officer in Charge, UNMIL/CITS
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. Rudy Sanchez, Chief, Information and Communications Technology Division, DFS
Mr. Byung-Kun Min, Special Assistant to the USG-OIOS
Ms. Eleanor 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

CHIEF, PEACEKEEPING AUDIT SERVICE:

Eleanor Burns: Tel: +1.917.367.2797, Fax: +1.212.963.3388,
e-mail: burnse@un.org

EXECUTIVE SUMMARY

Audit of ICT governance and security management in UNMIL

OIOS conducted an audit of information and communications technology (ICT) governance and security management in UNMIL. 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.

OIOS found that in general, UNMIL had in place adequate controls supporting ICT operations and security management. These controls facilitated the governance of ICT resources and the development of the infrastructure in accordance with professional best practices. In particular, OIOS noted good controls in the following areas:

- (a) A "Results based budget" framework was developed for 2009-2010 with detailed strategic priorities and outputs;
- (b) An assessment of the performance of the ICT function documented the results of the service provided during the last year, together with the remedial actions planned for mitigating the risks identified;
- (c) Well structured and comprehensive performance reports were prepared by UNMIL/Communications and Information Technology Section (CITS), detailing the qualitative and quantitative results accomplished;
- (d) An integrated administrative support paper for the United Nations in Liberia had been prepared, indicating the ICT perspectives, positions, plans, patterns, and directions for the "One UN Project Initiative";
- (e) An information and communications technology review committee was in place, with defined terms of reference, periodically scheduled meetings, and records of decisions taken;
- (f) A detailed catalogue of services provided by UNMIL/CITS was in place, with updated information (including costs) as of July 2009;
- (g) A draft project plan for "Site security and configuration review" was developed to implement a standard security configuration of all ICT resources in the Mission; and
- (h) Mission specific initiatives have been launched to rationalize the use of ICT resources (i.e. desktop and printer replacements).

However, OIOS observed that UNMIL 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. In this regard, the following opportunities for improvement were noted:

- (a) Lack of an exit strategy and plan for transferring the ICT infrastructure and knowledge to the United Nations Country Team (UNCT) upon completion of the Mission's drawdown phase;
- (b) ICT procedures were not always updated;
- (c) Inadequate procedures and controls for the identification of risks;
- (d) A standard UN project management methodology was not implemented;
- (e) Incomplete implementation of procedures to support the service delivery control framework adopted by the Mission;
- (f) Incomplete data classification schema and undocumented information architecture;
- (g) Inadequate asset and inventory management controls;
- (h) Inadequate physical and environmental controls;
- (i) Weak access control procedures; and
- (j) Incomplete disaster recovery and business continuity plan.

TABLE OF CONTENTS

Chapter	Paragraphs
I. INTRODUCTION	1 - 8
II. AUDIT OBJECTIVES	9
III. AUDIT SCOPE AND METHODOLOGY	10
IV. AUDIT FINDINGS AND RECOMMENDATIONS	
A. Strategy and governance	11 - 21
B. Project management	22 - 27
C. Service management	28 - 39
D. Information architecture	40 - 43
E. Asset management	44 - 54
F. Security, disaster recovery, and continuity of operations	55 - 80
V. ACKNOWLEDGEMENT	81
ANNEX 1 - Status of Audit Recommendations	

I. INTRODUCTION

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

2. UNMIL was established by Security Council resolution 1509 (2003) of 19 September 2003 to support the implementation of the ceasefire agreement and the peace process; protect United Nations staff, facilities and civilians; support humanitarian and human rights activities; as well as assist in national security reform, including national police training and formation of a new, restructured military.

3. The Security Council extended, with its resolution 1840 (2008), the mandate of the Mission until 30 September 2010. Therefore, the mission is currently in drawdown phase.

4. The Mission is organized in four sectors covering 15 counties, with the Mission headquarters located in the capital, Monrovia. The mission strength as of 30 September 2009 was 11,519 total uniformed personnel, including 10,033 troops and 131 military observers; 1,355 police; supported by 476 international civilian personnel, 975 local staff.

5. The provision of ICT services include the operations and maintenance of an infrastructure comprising 79 routers, 122 servers, 2,404 desktop computers, 683 laptop computers, 594 printers, and 80 digital senders.

6. The financial resources for ICT at UNMIL, as documented in the report of the Advisory Committee on Administrative and Budgetary Questions (ACABQ) on the financial performance for the period from 1 July 2007 to 30 June 2008, and proposed budget for the period from 1 July 2009 to 30 June 2010 of UNMIL (A/63/746 Add. 8), are as follows:

Operation	2008-2009 Apportionment (in thousands of USD)
Communications	17,539.3
Information Technology	5,263.1

7. UNMIL is the lead agency for the "One UN initiative in Liberia". In June 2008, the first joint UN office opened in Voinjama, Lofa County, bringing together seven UN agencies (Food and Agriculture Organization, United Nations Development Programme, United Nations International Children's Fund, United Nations Population Fund, United Nations High Commissioner for Refugees, World Food Programme, and World Health Organization) and UNMIL under a Memorandum of Understanding. Under the "One UN initiative" the joint office concept is recognized as an important method in advancing integration and bringing the UN together to make the best possible use of resources such as power supply, fuel stations, information technology infrastructure, and security. UNMIL charges the joint office on a cost-reimbursable basis for services such as

cleaning, security, and communications (internet and telephone), as per UN rules and regulations.

8. Comments made by UNMIL are shown in *italics*.

II. AUDIT OBJECTIVES

9. The main objectives of the audit were to assess whether UNMIL had adequate and effective internal controls in place to:

- (a) Govern and manage ICT resources;
- (b) Identify and manage risks;
- (c) Define and assign clear roles, responsibilities, and reporting lines;
- (d) Plan, monitor, report, and improve operations;
- (e) Implement Mission specific policies and standard operating procedures;
- (f) Manage assets;
- (g) Manage projects and initiatives on the basis of standard management methodologies; and
- (h) Secure ICT resources, data, and activities.

III. AUDIT SCOPE AND METHODOLOGY

10. The audit was conducted at UNMIL. Interviews were held with officers in charge of the relevant services and functions within the Mission, and relevant documentation and systems were reviewed. Tests were conducted on the ICT infrastructure of the Mission, including a network vulnerability assessment, to confirm the adequacy and effectiveness of the control environment.

IV. AUDIT FINDINGS AND RECOMMENDATIONS

A. Strategy and governance

Lack of a documented exit strategy and plan to transfer the ICT infrastructure to the United Nations Country Team on completion of the withdrawal phase

11. A strategy should give direction and establish priorities for the investment and management of ICT resources. The strategy should be complemented by an ICT governance framework defining the distribution of the

decision-making rights and responsibilities among different offices in the organization, and also establishing procedures and mechanisms for implementing and monitoring the strategic decisions.

12. UNMIL developed a "Results based budget" framework for 2009-2010 with detailed strategic priorities and outputs, and a paper for integrated administrative support in Liberia. This paper indicated that UNMIL, along with the United Nations Country Team (UNCT), was planning a transition period for transferring the ICT infrastructure, support, and knowledge from the Mission to UNCT upon the liquidation of the Mission. However, this plan was not supported by a documented strategy and a detailed plan for the transfer of assets (i.e. ICT infrastructure) and knowledge to UNCT.

13. UNMIL/CITS has the responsibility to manage the ICT resources of the Mission and to implement the annual plan of work approved by the General Assembly. While its plan of work for 2009-2010 indicated that UNMIL/CITS intended to maintain its established staff levels until June 2010, as of the time of the audit (November 2009) there was no planned action for scaling-down the current resources with the planned liquidation phase of the Mission.

Recommendations 1 and 2

(1) UNMIL/Division of Administration should coordinate with the United Nations Country Team in Liberia the transfer of ICT infrastructure and knowledge to UNCT on completion of the liquidation phase.

(2) As part of the liquidation plan, UNMIL/CITS should document a human resources action plan that aligns current resource requirements with the expected decrease in staffing capacity as a result of the Mission drawdown.

14. *UNMIL accepted recommendation 1 and stated that cross-training and capacity building have been already taken into consideration and are part of the Memorandum of Understanding (MOU) between Agencies and UNMIL. Recommendation 1 remains open pending receipt of the MOU established between UNMIL and Agencies documenting how the cross-training and capacity building processes have been regulated.*

15. *UNMIL accepted recommendation 2 and stated that, as of today, there is no liquidation plan, and that the actual military drawdown has no impact on the CITS resource(s) requirement. Recommendation 2 remains open pending receipt of the needs assessment for CITS resources with regard to the planned liquidation phase of the mission.*

Documentation not updated

16. OIOS found that relevant documentation pertaining to the functioning of the ICT governance bodies and incident management procedures had not been

regularly updated. This condition was particularly evident in the following two cases:

(a) An “Information and communications technology review committee” was in place, with defined terms of reference. The Committee periodically scheduled meetings, and kept records of decisions taken. However, its terms of reference did not reflect the changes recently introduced in the ICT management framework issued by the Office of Information and Communications Technology (OICT) at United Nations Headquarters; and

(b) UNMIL/CITS developed monthly duty rosters with contact information in case of incident. However, since the list of points of contact was only partially defined, staff in the Mission was potentially exposed to the risk of being unable to contact key personnel in case of need.

Recommendations 3 and 4

(3) UNMIL/Division of Administration should update the terms of reference of the “Information and communications technology review committee” in accordance with the newly released OICT management framework.

(4) Recommendation: UNMIL/CITS should complete the monthly duty rosters with the details and contact information of all duty officers.

17. *UNMIL accepted recommendation 3. Recommendation 3 remains open pending receipt of the updated terms of reference of the “Information and communications technology review committee” in accordance with the newly released OICT management framework.*

18. *UNMIL accepted recommendation 4 and stated that all contact details of duty technicians have been updated and the practice of forwarding the CITS Duty Roster in the Daily ICT Status Report has been implemented. Based on the actions taken, recommendation 4 has been closed.*

Inadequate procedures and controls for risk assessment

19. Professional best practices require that organizations conduct periodic risk assessments to identify threats that could negatively impact their ICT operations and assets.

20. CITS had well structured and comprehensive performance reports for communications and information technology activities, detailing the qualitative and quantitative results accomplished, completed through periodic performance review of its services. However, this review did not include a risk assessment of the ICT infrastructure to identify risks to operations and

assets, and to devise remedial plans for the implementation of adequate mitigating controls.

Recommendation 5

(5) UNMIL/CITS should develop a risk assessment methodology for conducting regular assessments of ICT risks and implement remedial actions for their mitigation.

21. *UNMIL accepted recommendation 5 and stated that a risk assessment methodology is being drafted with a five-step risk assessment: i) Ascertain the risk score; ii) Create the risk profile (strategic, operational, financial); iii) Modify the contributing risk characteristics; iv) Allocate test resources; and v) Create a risk database. Following this document, a risk-based audit plan will be drafted. Recommendation 5 remains open pending receipt of the risk assessment methodology developed by UNMIL.*

B. Project management

Lack of a standard project management methodology

22. 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) of the Department of Field Support indicated in its "vision paper" for the activities 2009-2010 that the methodology "Project in a controlled environment version 2 or PRINCE 2" was the standard project management methodology for DFS. However, OIOS found no evidence that this methodology had been formally implemented in UNMIL.

Recommendation 6

(6) UNMIL/CITS should formally implement the requirements of the UN standard ICT methodology (Prince-2) to prepare, review, approve, and manage ICT projects and initiatives through documentation of standard operating procedures and the training of staff in the use of the standard methodology (Prince-2).

23. *UNMIL accepted recommendation 6 and stated that training for 10 CITS staff members (Unit supervisors) is budgeted and confirmed. Following this training, CITS project and initiative will be managed with the use of Prince2 principles. Recommendation 6 remains open pending receipt by OIOS that CITS staff members have been trained on the standard project management methodology (Prince-2).*

Segregation of duties

24. Segregation of duties in the ICT environment addresses the need to separate incompatible functions. When these functions can't be fully segregated,

compensating controls should be established. OIOS found that while the Mission had a vacant position for project coordinator, one staff member was responsible for both project management and application development, with no compensating controls being implemented to mitigate the potential risks arising from this condition.

25. UNMIL acknowledged the need to maintain proper segregation between project and application management. In this regard, UNMIL clarified that in line with DFS/NYHQ recommendation, CITS does not develop any major application. Only few minor are being developed and do not require as such a dedicated project manager. However, UNMIL confirmed that in case of medium/major development, responsibilities between project management and application development will be segregated. Based on the clarifications provided by UNMIL, OIOS is not issuing any recommendation on this matter.

Lack of procedures for documenting user requirements

26. OIOS noted that application development requests had to be reviewed /approved by the ICT Review Committee (ICTRC) before starting the application development project. Business cases were prepared and reviewed locally and by New York Headquarters as required in the HQ Directive 2005-HQ-047303. However, there were no standard processes and methodology in place to document the ICT requirements of functional users.

Recommendation 7

(7) UNMIL/CITS should develop and implement standard operating procedures to enable the documentation of functional users' requirements.

27. *UNMIL did not accept recommendation 7, stating that functional user's requirements are established with the use of the high level business case template.* OIOS is unable to accept this response because the high level business case template provides justification for undertaking the project, estimates the high-level costs of the project, identifies the risks and summarizes the benefits of the project. However, this template does not document the detailed functional user's requirements. Recommendation 7 remains open pending receipt of the standard operating procedures to document functional users' requirements in UNMIL.

C. Service management

Informal staffing arrangements for the service desk

28. Formalized and defined assignment of responsibilities clarifies expectations and strengthens accountability of actions undertaken. The UNMIL service desk was staffed with two military personnel who addressed service call requests from users. However, the involvement of military personnel as support staff in the service desk was not formalized. Given the volume of calls (summarized in the table below), the unplanned termination of this informal

arrangement could expose the Mission to the risk of not being able to address critical requests for services.

Table 1: Analysis of service calls over 3 months

Month (2009)	Total Calls Answered	Number of calls taken by Military personnel	% of total calls
July	1280	1255	98%
August	1481	642	43%
September	1913	551	29%

Recommendation 8

(8) UNMIL/Division of Administration should formalize the arrangement for using military officers to support the service desk through a formal memorandum of understanding (MOU). The MOU should clearly define the responsibilities of the officers and specify termination requirements to avoid loss of service provision.

29. *UNMIL accepted recommendation 8 and stated that the integration and co-location of the military within Service Desk was an idea that was approved by G6 and CITS in November 2008. The objective was to be able to have 1st line resource who would represent and address military issues – the initiative would improve communication with the military, and the embedded officer(s) would understand/follow up, convey/explain ICT issues -including speak/understand a different language (Bengali for example). To date there have been no problems with this arrangement. A formalized MOU shall be prepared and submitted for approval. Recommendation 8 remains open pending receipt of the approved MOU formalizing the arrangement for using military officers in support of the service desk.*

Lack of service and operating level agreements

30. The provision of ICT services between providers and receivers is usually regulated on the basis of service level agreements (SLAs) and operating level agreements (OLAs). These agreements offer a structured approach with pre-defined terms and conditions for managing expectations and measuring performance. UNMIL/CITS did not have OLAs in place regulating its relationship with the United Nations Logistics Base (UNLB), its main provider of ICT services (i.e. for DFS enterprise wide applications, such as Lotus Notes email service), and SLAs with its own user community represented by the substantive and support offices within UNMIL.

Recommendation 9

(9) UNMIL/CITS should develop and implement service level agreements with all supported offices, and also with the United Nations Logistics Base.

31. UNMIL accepted recommendation 9 and stated that mission SLA/OLA documents will be drafted and signed off. SLA for the new i-Need CRM is in Draft. There are SLA(s) for Mercury and Galileo with UNLB. Strictly speaking, UNLB does not have SLAs with the missions but there is a Service Delivery Standard in terms of resolution time and incident categorization which UNMIL uses as the basis for the provision of service support from the hub. Recommendation 9 remains open pending receipt of the documented and approved service level agreements between UNMIL, supported offices, and UNLB.

Undefined performance indicators

32. UNMIL/CITS has a detailed catalogue of services provided, completed with updated information (including costs) as of July 2009, and service desk reports provided relevant information about the state of the ICT managed environment. UNMIL/CITS generated weekly and monthly service desk reports. However, these reports were not compared against key performance indicators (KPIs) to measure the effectiveness and efficiency of the service provided. Furthermore, operational data were not collected to provide a summary of:

- (a) The types of service calls received; and
- (b) How service desk queries were received (telephone, email, etc).

33. User surveys can provide valuable insight into how services are perceived and also offer the opportunity to highlight the value that CITS adds to ICT service provision within UNMIL. UNMIL/CITS had not conducted any recent satisfaction survey of its user community to measure the effectiveness of service provision within its user community.

Recommendations 10 and 11

(10) UNMIL/CITS should update its service monitoring procedures and benchmark quantitative and qualitative metrics against pre-defined key performance indicators. Furthermore, as part of the service monitoring process, operational data should be collected providing a summary of: (a) The types of service calls received; and (b) How service desk queries are received.

(11) UNMIL/CITS should periodically undertake a survey of its user community.

34. UNMIL partially accepted recommendation 10 and stated that Network Operations Center (NOC), embedded within CITS Service Desk, compiles and generates ICT Service Status Reports every day with quantitative metrics against pre-defined Key Performance Indicators. The mailing list recipients of this report include the Chief-ISS, DMS and CAS. Qualitatively, UNMIL/CITS is using an off-the-shelf automation help desk ticket system, called "HelpStar 9.0". UNMIL further indicated that logging 'How service desk queries are received' is not

possible in the current version. However, this option is available in the DFS i-Need CRM Help Desk web application which UNMIL is a pilot. In i-Need the Service Request Type allows the correct ITIL process to be selected from a predefined drop down menu, as follows: i) IM for Incident Management, ii) RFS for Request for Service, and iii) PM for Problem Management. The Service Request form in the new application includes a source field- drop-down with the option to select - e-mail, phone, fax, web or walk-in, etc to log how the call was received. Recommendation 10 remains open pending receipt of documentation showing the configuration and use in UNIMIL of the new “i-Need” system for monitoring and measuring performance of ICT services.

35. *UNMIL accepted recommendation 11 and stated that CITS currently tracks the ‘hard’ measures of service desk performance via KPI metrics. Importance to assess the ‘soft’ measures is noted. Customer Surveys will be conducted twice a year starting May 2010. Furthermore, electronic surveys shall be automated via the i-Need Application in the future. Recommendation 11 remains open pending receipt of the results of the customer surveys conducted in May 2010, and those electronically performed with the use of the application “i-Need”.*

Incomplete implementation of the control framework for service management

36. UNMIL/CITS adopted a control framework (Information technology infrastructure library or ITIL) for its service management activities. This framework contains best practices for developing a systematic approach to the management of ICT service provision and support. Specifically, the framework aims at: i) Providing a quality approach to service delivery; ii) Increase productivity; iii) Increase customer satisfaction; iv) Minimize risks; v) Reduce costs; and vi) Improve communication between ICT service providers and users. UNMIL/CITS stated that it used this framework for managing its service delivery activities. However, OIOS noted that UNMIL/CITS did not establish document procedures in line with the requirements of the control framework for service delivery. For example:

- (a) UNMIL/CITS did not implement incident management procedures, and lacked formalized event reporting procedures to report data about security problems and weaknesses, such as virus attacks;
- (b) Change management procedures were not documented. This condition could lead to unauthorized changes, and ineffective and inconsistent use of resources. An assessment of the risks and security impacts of proposed changes were not undertaken, potentially leading to the implementation of inconsistent security controls;
- (c) UNMIL/CITS did not have a “configuration management database (CMDB)” to maintain a baseline of the Mission’s software and systems, and to track control changes to installed applications; and
- (d) UNMIL/CITS did not document release management procedures for quality assurance, deployment and support of software releases.

37. In addition, while UNMIL/CITS launched mission specific initiatives to rationalize the use of ICT resources (i.e. desktop and printer replacements), and implemented tools for monitoring capacity requirements on current usage, it did not use this data to determine future capacity requirements and prevent inefficiencies associated with either under-utilized resources or unmet user demand.

Recommendations 12 and 13

(12) UNMIL/CITS should develop ICT service processes and document service procedures in line with its standard service delivery framework (Infrastructure Technology Information Library).

(13) UNMIL/CITS should define in its capacity monitoring procedures the future capacity requirements benchmarked against available resources.

38. *UNMIL accepted recommendation 12 and stated that a functional service desk is in place at UNMIL and is the single, first point of contact for ICT support. The "Help Star 9.0" ticket system is used by all CITS units to manage user and client ICT requests such as standard changes, questions, complaints, comments, difficulties and queries and to report non major incidents.. Incident categorization, prioritization, service management reports are handled in this application. For access to systems, including Galileo, Mercury, etc. in which approval is required, the e-request application is used. SOPs and documentation have been prepared on the work flow of the two systems. However, the applications are not fully ITIL compliant. In addition problem management and change management workflow processes are not available in Help Star 9.0 automation tool. Problem Management functionality will be available in the "iNeed" DFS CRM application which will also have an interface to the e-Request application. UNMIL/CITS is also in the process of maintaining a centralized repository of its Configuration Management documents on the share drive S:\CITS Documents. Automation of the Configuration Management will be provided in a future release of "iNeed" CRM. Presently, documentation and SOPs for the DFS "iNeed" CRM application have been provided including access to online training to the ITIL compliant system. Training in ITIL intermediate level and foundation is planned this year. In 2008, 16 CITS staff participated in the ITIL Foundation course in service management and 10 will participate in early June in the foundation course "+ ITIL". Recommendation 12 remains open pending receipt of the documented procedures developed in accordance with the standard service delivery framework ITIL and supported by the application "i-Need".*

39. *UNMIL accepted recommendation 13 and stated that capacity planning shall include three elements: i) Determine capacity requirement; ii) Analyze current capacity; and iii) Plan for future capacity. The last element is dependent on the two first ones which have been implemented recently, and is being developed. In particular, and in line with recommendation 2, CITS will forecast*

expected workload for a particular time (i.e. liquidation, downsizing) and translate into technical requirement necessary to maintain the support at a level that satisfies user demand. Thresholds will also be defined to represent utilization levels requiring action necessary to change capacity, for mitigation the risk of capacity bottlenecks. Recommendation 13 remains open pending receipt of the documented forecasts of UNMIL's ICT-related requirements.

D. Information architecture

Incomplete data classification schema and undocumented information architecture

40. 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. In this regard, the Information Management Unit in UNMIL developed only data classification schema for paper records.

41. 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. UNMIL did not document its information architecture for facilitating the understanding of the flow of information held within its different information systems, and it indicated that is awaiting the implementation of the organization-wide enterprise content management (ECM) system.

Recommendations 14 and 15

(14) UNMIL/Division of Administration should implement the DPKO policy directive entitled "Records Management" (updated in December 2007) for developing a taxonomy of information in line with ST/SGB/2007 on Information Sensitivity, Classification and Handling.

(15) Pending the implementation of the enterprise wide content management system (ECM), UNMIL/CITS should document the information architecture of its applications and systems to monitor the flow of information among its core processes.

42. *UNMIL accepted recommendation 14 and stated that its Information Management Unit (IMU) is in the process of implementing ST/SGB/2007/5 on "Record keeping and management of United Nations Archives" together with the DPKO DFS Policy Directive on Records Management as directed by the Audit Report AP2009/626/11 on "Records Management in UNMIL". The record management focal points network has been established and trained, the inventory of UNMIL records is undergoing (deadline 30 June), with the full implementation of the file classification scheme scheduled for December 2010. The recommendations to comply with ST/SGB/2007/6 and UNMIL AI 2007/001 with*

regard to handling of sensitive information, and to strengthen the controls over code cables and Notes Verbale, from the same audit, have already been closed. However, UNMIL/IMU is still improving the implementation of the Bulletin's provisions by developing new training sessions for different groups of staff members dealing with sensitive information. Also, because of the absence of a record-keeping system in the Mission, CITS together with IMU are in process of establishing a shared-drive for management of internally-drafted confidential and strictly confidential communications. Recommendation 14 remains open pending receipt of documentation showing that UNMIL/IMU has completed the implementation of the provisions established by ST/SGB/2007/5.

43. UNMIL did not accept recommendation 15, stating that currently CITS has documentation for end-user manual, technical design manuals and administrative user guides for locally developed applications and systems. The Applications Unit also maintains a spreadsheet of all the applications showing the inter-dependencies with other applications. The inter-dependency spreadsheet shows the inbound and outbound data (Information) amongst the various applications. Presently UNMIL CITS does not embark on major application/system developments since the centralization of development in Entebbe and UN HQ. In this regard there is no need to incorporate minor information architecture of the minor application design customizations in the ECM. OIOS takes note of the clarifications provided by UNMIL and will close recommendation 15 upon receipt of the documentation showing the inter-dependencies between applications, including the inbound and outbound data flow amongst them.

E. Asset management

Inadequate asset and inventory management controls

44. Inventories of assets assist with the traceability of ICT equipment through the different stages of their lifetime up to the final disposal.

45. While UNMIL had in place a process for monitoring inventory movement, there were gaps within the ICT inventory control environment, particularly evident when equipment left the UNMIL/CITS warehouse. UNMIL/CITS equipment was often held at other locations outside the main warehouse such as workshops, other Mission's Sectors, the Starbase, and Headquarters. All these locations were not included in the inventory count and instead considered as part of the central UNMIL/CITS warehouse inventory management procedure.

Recommendation 16

(16) UNMIL/CITS should implement a process for tracking all ICT equipment held in the warehouse and other locations throughout the Mission. Furthermore, procedures should be developed and implemented to ensure that damaged and obsolete equipment are returned to the warehouse for disposal.

46. UNMIL accepted recommendation 16 and stated that the recommendation on tracking of assets held in warehouse and other location was already addressed in BOA/UNMIL/2007/138. All ICT holdings held in the warehouse and other locations throughout the Mission are tracked through annual physical verifications, data collected is recorded in physical verification (PV) sheets and Galileo Inventory System updated accordingly. Discrepancies encountered between physical verifications and books are recorded and addressed adequately to ensure inventory accuracy. UNMIL two last warehouse PVs have shown 100% accuracy. Regular PVs are conducted as required at any time of the year. This procedure was implemented since 2005 and AMU is ensuring that at least two official physical verifications take place during the year for Non-Expendables and at least one for Expendable property. Additionally, a new SOP has been developed for movement of assets from warehouses to various locations, instating that CMR and Movement Control (MovCON) offices are to be used for all movements. Some equipment was left out of the warehouse in some office due to re-arrangement/cleaning of the warehouse. The warehouse is now fully "operational" and all assets are duly back and described as "in stock". All damaged and obsolete equipment returned to the warehouse are placed daily/weekly in dedicated containers following technical and inventory inspections every Friday. Procedure was developed and implemented in 2007. Recommendation 16 remains open pending receipt of the new standard operating procedure developed in UNMIL to track the movement of assets from warehouses to various locations, and for the disposal of damaged or obsolete equipment.

Hardware failures

47. The requisition of computer equipment to be used in the Mission's locations should take into account their particular climate and operating conditions. In this regard, OIOS noted that ICT equipment procured by the Mission was frequently subject to failure due to their inability to withstand the Mission's climatic conditions.

48. CITS staff deployed in the various Missions would be the best source of input to DFS New York Headquarters for defining the standard specifications of procuring equipment intended for use in the Mission.

Recommendation 17

(17) UNMIL/CITS should define the specific climatic requirements in the requisitions of its computing equipment sent to DFS/ New York Headquarters.

49. UNMIL did not accept recommendation 17, stating that computing equipment purchased by UN through system contracts are for use in standard office environment and covers 99% of the applications in the field as UN staff works mostly in climate controlled areas. Every RFP for computing equipment states: "the offered products shall be heavy duty, highly reliable and operate normally under harsh environmental conditions". Should the mission have a

specific requirement for "ruggedized" equipment it could be approved for a "spot" purchase under the understanding that such requirement brings a premium price (100 to 500% more). ICTD haven't received similar request from other missions but should this requirement be DFS wide, ICTD will consider the establishment of a system contract. OIOS is unable to accept UNMIL's response, since the presence of standard requirements in the request for proposals did not prevent the high rate of hardware failures registered in the Mission. OIOS was informed that the cause of these failures was due to the climatic conditions in which the hardware is used. Therefore, OIOS is of the opinion that the causes of this high rate of failures should be adequately documented and input provided to DFS to prevent future recurrence of this problem and waste of resources (i.e. costs associated with the repair and replacement of the equipment). Recommendation 17 remains open pending receipt of evidence documenting the actions taken by UNMIL with regard to the high rate of hardware failures.

Disposal of computer equipment

50. The disposal of computer equipment should be conducted on the basis of pre-defined actions to prevent the risks of: (a) Having a negative impact on the environment; (b) Lead to unauthorised disclosure of sensitive data; and (c) Losing Mission's assets.

51. During a visit to the radio room, OIOS observed that damaged equipment (i.e. Uninterruptible Power Source) had not been returned back to the assets warehouse for disposal, but were left lying in piles under the stairs of the building. In addition, an ICT programme review report highlighted the following issues:

(a) UNMIL ICT had a surge of obsolete equipment. This problem had been recognized and obsolescence management was included in the work plan for 09/10;

(b) A problem with excessive numbers of desktop printers, associated costs and shortage of cartridges. The Mission documented a new policy on the rationalization of printers; and

(c) A problem with a high stock of expendable line items, included in the list of issues to be reviewed during the 09/10 work plan.

52. In addition, UNMIL lacked a formalized process to protect the Mission against the risks of disposing or re-using computing equipment. 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 its disposal. Furthermore, laptops were currently not being re-configured (i.e. re-imaged) before being assigned to new users.

Recommendations 18 and 19

(18) UNMIL/CITS should continue to monitor and put in place measures to mitigate the problems with regard to obsolescence, excessive printers, and high stock of expendable line items.

(19) UNMIL/CITS should develop and implement procedures for ensuring that as part of the disposal process of assets, adequate actions are taken to remove all data stored within any device.

53. *UNMIL accepted recommendation 18 and stated that it will continue monitoring this process.* Recommendation 18 remains open pending receipt of documentation showing the measures put in place in UNMIL to mitigate the problems with regard to obsolescence, excessive printers, and high stock of expendable line items.

54. *UNMIL accepted recommendation 19 and stated that all computers to be written-off will be inspected and tagged to ensure that all data have been removed. For laptops, no hand-over from users to users will be accepted. All laptops before being reassigned will have to go through the warehouse where re-imaging will be done.* Recommendation 19 remains open pending receipt of the documented procedures established in UNMIL for the disposal of assets and the removal of data stored within.

F. Security, disaster recovery and continuity of ICT operations

Inadequate physical and environmental controls

55. Adequate physical and environmental security controls should provide a physical barrier as a preventive measure against threats to an organization's information resource. UNMIL 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 UNMIL information and assets. Table 2 lists the gaps identified:

Table 2. List of gaps in the physical controls	
Location	Gaps
Data Center/Server Room in Mission Headquarters	<ul style="list-style-type: none"> • No fire extinguisher inside server room / data center. • Electrical cables on the outer back wall of the server room (behind the PAP building) were not adequately protected against physical security and environmental threats.
Radio Server room in Mission Headquarters	<ul style="list-style-type: none"> • Wooden door (not metallic door) installed at second entrance to Radio server room. • Powder fire extinguisher was distantly located outside the radio server room. • Water leakage in the radio server room, with the source not identified. • Server racks and other equipment in located in the server room were not raised as per standard procedure. • The physical barrier represented by the entrance door in the radio server room (metallic door) could have been bypassed by coming in the room from the upper floor using an internal staircase.
UPS room in Mission Headquarters	<ul style="list-style-type: none"> • The uninterruptible power supply (UPS) had a high failure rate, probably due to poor environmental conditions and lack of diagnostic software (not currently installed and enabled) in each UPS unit. • The location of the UPS room on the ground floor of the building in UNMIL MHQ PAP made it susceptible to unauthorized access. • The failed UPS units were just stored under the staircase in a common area that was easily accessible, posing also a health and safety issue.
UNMIL/CITS equipment warehouse	<ul style="list-style-type: none"> • The warehouse was subject to water leaks when it rained, potentially causing damage to equipment. • Although CCTV cameras were installed in the UNMIL/CITS warehouse, these were not monitored.

Recommendation 20

(20) UNMIL/CITS should implement physical and environmental controls in line with industry best practices to safeguard Mission information and equipment.

56. UNMIL accepted recommendation 20 and stated that: (i) Data center request for fire extinguisher to be placed inside the server room is done. It is to be noted that this concern is applicable only to one data center.. Additionally, a fire extinguisher is available in front of the door of the data center. Risks are therefore mitigated. The electrical cables referred to are placed inside AC conduits. Request has been done to close the conduits with PVC cover; (ii) Radio Server room: The radio server room referred in the recommendation is the equipment room of the Public Information Office (PIO). CITS forwarded the audit comment to PIO and will provide guidance to respond to the recommendations; (iii) UPS Room: UNMIL/CITS has received 4 new UPS of high capacity to replace

the bank of old ones in the two data center. Those new UPS are centrally managed through diagnostic software. Regarding the recommendation related to failed UPS Units as well as the possibility of unauthorized access to UPS room, this refers to equipment belonging and managed by PIO. Those recommendations have been transmitted to PIO; and (iv) UNMIL/CITS Equipment warehouse: Request to repair the roof has been done. In the same time, equipment has been removed from the area affected by the leak. CCTV is monitored. Recommendation 20 remains open pending receipt of a documented confirmation that all the weaknesses identified in the physical and environmental controls in UNMIL have been addressed.

Inadequate handling of confidential documents

57. The handling of confidential documents should be performed in accordance with established procedures and controls to avoid their duplication and secure their distribution and storage.

58. OIOS noted that Mission code cables were duplicated and stored in the code cable room, exposing them to the risk of loss of confidentiality. Additionally, the audit found that the shredder used in the code cable room was not adequate (i.e. a 'strip shredder' that cuts paper in long strips that could be easily reassembled) for performing the disposal of confidential documents.

Recommendations 21 and 22

(21) UNMIL/CITS should amend its internal procedure for handling code cables to ensure their confidentiality and integrity.

(22) UNMIL/CITS should replace the shredding machines installed in the code cable unit with equipment that shred paper into confetti-like pieces.

59. *UNMIL accepted recommendation 21 and stated that the office of Chief of Staff is currently reviewing the policy/procedures. Recommendation 21 remains open pending receipt of the new procedures for handling code cables.*

60. *UNMIL accepted recommendation 22 and stated that a new shredder machine (cross-cutting) has been provided to the Communication Centre. Based on the action taken by UNMIL, recommendation 22 has been closed.*

Security of mobile computing devices

61. The use of mobile computing devices should be safeguarded with precautionary measures to prevent unauthorised access, theft, data loss, and virus infections. UNMIL/CITS lacked a formalized process for securing the mobile computing devices it supported. OIOS noted that hard drives were not being encrypted on the laptops, exposing them to the risks of unauthorized access, and loss of confidentiality, integrity and availability of information assets.

62. In addition, UNMIL laptops did not receive regular anti-virus updates (Symantec anti-virus server) because these machines were often offline during the time when the anti-virus server “pushed” signature updates to the systems on the UNMIL network. This condition could result in the loss of confidentiality, integrity and availability of information assets through malicious code infection.

Recommendations 23 and 24

(23) UNMIL/CITS should define and implement more stringent security measures for laptops (e.g. encryption of laptop hard-drive and removable media).

(24) UNMIL/CITS should configure laptops to “pull” anti-virus signature updates from the “Symantec anti-virus” server or give laptop users the ability to manually update their anti-virus signatures from the Internet on a regular basis.

63. *UNMIL accepted recommendation 23 and stated that it is foreseen to use Windows 7 which integrates HDD encryption.* Recommendation 23 remains open pending receipt of documentation showing that more stringent security measures have been implemented.

64. *UNMIL accepted recommendation 24 and stated that workstations have been reconfigured to automatically pull new antivirus updates from the server.* Based on the actions taken in UNMIL, recommendation 24 has been closed.

Information security controls

65. Professional best practices require that organizations define information security policies and assign specific responsibilities for their implementation, monitoring, and compliance to designated officers.

66. In its report titled “ICT programme review”, UNMIL/CITS identified several actions to be completed during the period 2009-2010 in the area of information security in a report titled. These actions included:

- (a) Conduct a security audit or penetration tests;
- (b) Hire an IT security officer (reporting to the Division of Mission Support); and
- (c) Issue a comprehensive security policy.

67. However, as of the time of the audit (November 2009), OIOS noted that none of the above listed actions had been implemented. These conditions could potentially lead to: a) Gaps in the effectiveness of security controls; b) Inconsistent implementation of security controls; and c) Inability to detect threats or vulnerabilities.

Recommendation 25

(25) UNMIL/CITS should develop an information security policy and appoint an information security officer for its implementation and monitoring. Furthermore, UNMIL/CITS should ensure that periodic vulnerability tests of the Mission's network are regularly conducted.

68. *UNMIL accepted recommendation 25 and stated that: i) A post, budgeted at P2 level, has been reserved for the information security function, and short-listed candidates are being reviewed; ii) The ICT control access policy (DPKO Policy Directive) is the reference Information Security Policy; and iii) Vulnerability tests will be conducted.* Recommendation 25 remains open pending receipt of documentation showing that the ICT security officer has been appointed, a comprehensive security policy has been developed in accordance with DPKO Policy Directive, and periodic vulnerability tests of the Mission's network are conducted.

Weak access control procedures

69. Access to applications and systems should be granted on a need-to-know basis, based on minimum requirements for passwords length and complexity, and subject to regular monitoring procedures to ensure the termination of accounts related to staff that is not longer on duty.

Dormant accounts

70. UNMIL had approximately 3,400 user identification accounts (user IDs) in its "Windows active directory" (excluding system's IDs). This high number of user IDs appeared to be more than the number of authorized network users working in UNMIL. Therefore, this condition indicated that several "dormant" user IDs had not been removed from the Windows active directory, exposing the Mission to the risk of unauthorized access and loss of confidentiality of information resources.

Recommendation 26

(26) UNMIL/CITS should perform regular reviews of users' access to all critical servers, applications and services, and delete user accounts assigned to staff no longer assigned to the Mission.

71. *UNMIL accepted recommendation 26 and stated that CITS scans all accounts on a weekly basis to notify and deactivate accounts that have no activity during the last 90 days. Two weeks after this notification, the account is removed. As a consequence of those new weekly screening, total number of accounts is now 2914, i.e. almost 400 less than at the time of the audit.* Based on the actions taken in UNMIL, recommendation 26 has been closed.

Lack of enforcement of minimum requirements for passwords

72. The password management system established in UNMIL was ineffective because there were no mechanisms in place to enforce changes of default passwords and the subsequent selection of strong passwords by users in Lotus Notes and other critical applications. OIOS found that:

- (a) Users were not required to maintain strong passwords (i.e. the mechanism to force selection of strong passwords by users was not enabled on the production servers);
- (b) There was no consistency in forcing regular password changes for users after 90 days; and
- (c) Default passwords were still being used for user and administrator accounts on some critical equipment (e.g. the microwave network generator chargers).

Recommendation 27:

(27) UNMIL/CITS should implement a mechanism to consistently require users to: a) Change default passwords in Lotus Notes; b) Change passwords every 90 days on all servers; and c) Select strong passwords consisting of numbers, different case characters and symbols.

73. *UNMIL accepted recommendation 27 and stated that a comprehensive policy has been drafted and is being submitted to UNMIL/Administration. By implementing this policy, the actions included in point a) b) and c) will be covered. Recommendation 27 remains open pending receipt of the approved password policy.*

Inadequate access to helpdesk application

74. OIOS noted that users of the current helpdesk application (Helpstar) were not given unique user ID's, and did not have unique passwords to access the application. Also, the ability to close tickets within the application was not restricted. This condition weakened the accountability and the integrity of the information contained within the application.

Recommendation 28

(28) UNMIL/CITS should configure more stringent access and password controls in its customer relationship application ("Helpstar" and the future "i-Need"), ensuring that users receive unique account identifiers.

75. *UNMIL accepted recommendation 28 and stated that although there are limited licenses for the application "HelpStar" (27 in total), each of the CITS Units including regions have an assigned group generic ID and password, and*

are responsible for their queues that they manage. Despite the disadvantages of using a generic ID and password, technicians are encouraged to sign off service requests in their own names. "HelpStar" is linked to the Active Directory, and technicians select their names from the Windows directory and update the status of jobs they are working on in free form text and flag resolved jobs as In Progress or Completed. In normal circumstances, Service Desk staff monitor/check the application for tickets with completed status and close the call/job after confirming with the end-user satisfactory work completion. Due to the fact that UNMIL is moving to the i-Need application, and has participated in the User Functional Testing (UFT) and User Acceptance Testing (UAT) of the DFS CRM throughout 2009, no additional licenses were procured or further development/customization made on the "HelpStar" application. Nevertheless SOPs/documentation for the proper use of the application are in place. In the case of Self-Help access over the intranet, end-users can open a ticket using unique login credentials pulled from Windows Active Directory (i.e. <first and last name>). However, end users are assigned a common password <helpstar> for the Intranet Self-service option. In the new DFS iNeed CRM application, each technician will have a unique ID and password, and belong to a particular service group. Only technicians who are members of the Service Desk group shall be able to close tickets that have been resolved and/or re-open closed tickets. This will ease tracking of each Technician's involvement in the resolution of any service request. Recommendation 28 remains open pending receipt of documented evidence confirming that access to the customer relationship management application in use in UNMIL (i.e. iNeed) is granted only on the basis of unique credentials and identifiers.

Incomplete disaster recovery and business continuity plans

76. Regular tests of the business continuity and disaster recovery plans should be conducted for validating the reliability of the supporting documentation and processes, and also train and prepare personnel using a simulation of a disaster.

77. UNMIL developed an ICT disaster recovery plan with 5 scenarios. However, simulation tests of the whole plan were not conducted (limited forced tests were completed during power interruptions). In addition, UNMIL lacked a business continuity plan with the identification of essential staff in each functional area.

78. The disaster recovery and business continuity plan of the Mission was focused only on the recovery of ICT assets in the event of a disaster and did not contain the necessary information to ensure adequate continuation of the business processes.

Recommendations 29 and 30

(29) UNMIL/CITS should undertake periodic tests of its information and communications disaster recovery plan.

(30) UNMIL/CITS in coordination with representatives of the substantive and support offices should complete the business continuity plan of the Mission with essential information related to “who, how, and where” each functional area will resume and continue their operation in case of a disaster. Upon completion of this task, UNMIL/CITS should update the references to its disaster recovery and business continuity plans by formally referencing two distinct documents, i.e.: a) The “Disaster Recovery Plan”; and b) The “Business Continuity Plan”.

79. *UNMIL accepted recommendation 29 and stated that a periodic test plan document is being drafted and will be submitted to New-York HQ/DRBC Team for review and approval. Recommendation 29 remains open pending receipt of documented confirmation that the plan for periodic tests of the disaster recovery measures has been approved and tests implemented.*

80. *UNMIL accepted recommendation 30 and stated that CITS welcomes the development of a Mission Business Continuity plan at the Mission level and will work with the Mission Administrative staff for their related portion of a High Level Mission Business Continuity plan (BC Plan), once a Mission BC plan is in place the CITS disaster recovery plan document and procedures will be adjusted and tested accordingly. Recommendation 30 remains open pending receipt of the documented and approved business continuity plan aligned with the disaster recovery plan of the mission.*

V. ACKNOWLEDGEMENT

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

STATUS OF AUDIT RECOMMENDATIONS

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
1	UNMIL/Division of Administration should coordinate with the UNCT in Liberia the transfer of ICT infrastructure and knowledge to UNCT on completion of the liquidation phase.	Strategy	High	O	Submit copy of the Memorandum of Understanding (MOU) between UNMIL and United Nations Agencies documenting how the cross-training and capacity building processes are regulated.	Not provided
2	As part of the liquidation plan, UNMIL/CITS should document a human resources action plan that aligns current resource requirements with the expected decrease in staffing capacity as a result of the Mission drawdown.	Governance	High	O	Submit evidence documenting the needs assessment completed for CITS resources with regard to the planned liquidation phase of the mission	Not provided
3	UNMIL/Division of Administration should update the terms of reference of the "Information and communications technology review committee" in accordance with the newly released OICT management framework.	Governance	Medium		Submit copy of the updated terms of reference of the "Information and communications technology review committee" in accordance with the newly released OICT management framework	Not provided
4	UNMIL/CITS should complete the monthly duty rosters with the details and contact information of all duty officers.	Operational	Medium	C	Based on the actions taken by UNMIL in updating the details of the duty rosters this recommendation is closed.	Implemented
5	UNMIL/CITS should develop a risk assessment methodology for conducting regular assessments of ICT risks and implement remedial actions for their mitigation.	Governance	Medium	O	Submit copy of the ICT risk assessment methodology completed in UNMIL.	August 2010
6	UNMIL/CITS should formally implement the requirements of the UN standard ICT methodology (Prince-2) to prepare, review, approve, and manage ICT projects and initiatives through documentation of standard operating procedures and the training of staff in the use of the standard methodology (Prince-2).	Operational	Medium	O	Submit documented evidence that UNMIL ICT staff members have been trained on the standard project management methodology (Prince-2).	May 2010

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
7	UNMIL/CITS should develop and implement standard operating procedures to enable the documentation of functional users' requirements.	Operational	Medium	0	Submit copy of the standard operating procedures for documenting functional users' requirements in UNMIL.	Not provided
8	UNMIL/Division of Administration should formalize the arrangement for using military officers to support the service desk through a formal memorandum of understanding (MOU). The MOU should clearly define the responsibilities of the officers and specify termination requirements to avoid loss of service provision.	Governance	High	0	Submit copy of the approved Memorandum of Understanding (MOU) formalizing the arrangement for using military officers in support of the service desk.	May 2010
9	UNMIL/CITS should develop and implement service level agreements with all supported offices, and also with the United Nations Logistics Base.	Operational	Medium	0	Submit copy of the documented and approved service level agreements between UNMIL, supported offices, and UNNLB.	June 2010
10	UNMIL/CITS should update its service monitoring procedures and benchmark quantitative and qualitative metrics against pre-defined key performance indicators. Furthermore, as part of the service monitoring process, operational data should be collected providing a summary of: (a) The types of service calls received; and (b) How service desk queries are received.	Operational	Medium	0	Submit evidence documenting the configuration and use in UNMIL of the new "i-Need" system for monitoring and measuring performance of ICT services.	May 2010
11	UNMIL/CITS should periodically undertake a survey of its user community.	Operational	Medium	0	Submit copy of the results of the customer surveys conducted in May 2010, and of those electronically performed with the use of the application "i-Need"	May 2010
12	UNMIL/CITS should develop ICT service processes and document service procedures in line with its standard service delivery framework (Infrastructure Technology Information Library, ITIL).	Operational	Medium	0	Submit copy of the procedures developed in accordance with the standard service delivery framework ITIL and supported by the application "i-Need".	Not provided

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
13	UNMIL/CITS should define in its capacity monitoring procedures the future capacity requirements benchmarked against available resources.	Operational	Medium	O	Submit copy of the documented forecasts of UNMIL ICT-related requirements.	31 December 2010
14	UNMIL/Division of Administration should implement the DPKO policy directive entitled "Records Management" (updated in December 2007) for developing a taxonomy of information in line with ST/SGB/2007 on Information Sensitivity, Classification and Handling.	Compliance	High	O	Submit evidence documenting that UNMIL/IMU has completed the implementation of the provisions established by ST/SGB/2007/5.	Not provided
15	Pending the implementation of the enterprise wide content management system (ECM), UNMIL/CITS should document the information architecture of its applications and systems to monitor the flow of information among its core processes.	Operational	Medium	O	Submit documentation showing the inter-dependencies between applications, including the inbound and outbound data flow amongst them	Not provided
16	UNMIL/CITS should implement a process for tracking all ICT equipment held in the warehouse and other locations throughout the Mission. Furthermore, procedures should be developed and implemented to ensure that damaged and obsolete equipment are returned to the warehouse for disposal.	Operational	Medium	O	Submit copy of the new standard operating procedure developed in UNMIL to track the movement of assets from warehouses to various locations, and for the disposal of damaged or obsolete equipment.	Not provided
17	UNMIL/CITS should define the specific climatic requirements in the requisitions of its computing equipment sent to DFS/ New York Headquarters.	Operational	Medium	O	Submit evidence documenting the actions taken by UNMIL with regard to the high rate of hardware failures and subsequent input submitted to NYHQ.	Not provided
18	UNMIL/CITS should continue to monitor and put in place measures to mitigate the problems with regard to obsolescence, excessive printers, and high stock of expendable line items.	Operational	Medium	O	Submit documented evidence of the measures put in place in UNMIL to mitigate the problems with regard to obsolescence, excessive printers, and high stock of expendable line items.	Not provided

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
19	UNMIL/CITS should develop and implement procedures for ensuring that as part of the disposal process of assets, adequate actions are taken to remove all data stored within any device.	Governance	High	O	Submit evidence of documented procedures established in UNMIL for the disposal of assets and the removal of data stored within.	July 2010
20	UNMIL/CITS should implement physical and environmental controls in line with industry best practices to safeguard Mission information and equipment.	Operational	Medium	O	Submit documented confirmation that all the weaknesses identified in the physical and environmental controls in UNMIL have been addressed.	Not provided
21	UNMIL/CITS should amend its internal procedure for handling code cables to ensure their confidentiality and integrity.	Operational	High	O	Submit copy of the new procedures for handling code cables in UNMIL.	June 2010
22	UNMIL/CITS should replace the shredding machines installed in the code cable unit with equipment that shred paper into confetti-like pieces.	Operational	Medium	C	Based on the actions taken in UNMIL for replacing the shredding machines, this recommendation is closed.	Implemented
23	UNMIL/CITS should define and implement more stringent security measures for laptops (e.g. encryption of laptop hard-drive and removable media).	Operational	Medium	O	Submit documented evidence confirming that more stringent security measures have been implemented for laptops.	Not provided
24	UNMIL/CITS should configure laptops to "pull" anti-virus signature updates from the "Symantec anti-virus" server or give laptop users the ability to manually update their anti-virus signatures from the Internet on a regular basis.	Operational	Medium	C	Based on the actions taken in UNMIL for re-configuration of the anti-virus software, this recommendation is closed.	Implemented
25	UNMIL/CITS should develop an information security policy and appoint an information security officer for its implementation and monitoring. Furthermore, UNMIL/CITS should ensure that periodic vulnerability tests of the Mission's network are regularly conducted.	Governance	High	O	Submit documented evidence confirming that the ICT security officer has been appointed, a comprehensive security policy has been developed in accordance with DPKO Policy Directive, and periodic vulnerability tests of the Mission's network are conducted.	Not provided

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
26	UNMIL/CITS should perform regular reviews of users' access to all critical servers, applications and services, and delete user accounts assigned to staff no longer assigned to the Mission.	Operational	Medium	C	Based on the actions taken in UNMIL with regard to the review of user's access, this recommendation is closed.	Implemented
27	UNMIL/CITS should implement a mechanism to consistently require users to: a) Change default passwords in Lotus Notes; b) Change passwords every 90 days on all servers; and c) Select strong passwords consisting of numbers, different case characters and symbols.	Operational	Medium	O	Submit copy of the approved password policy.	June 2010
28	UNMIL/CITS should configure more stringent access and password controls in its customer relationship application (Helpstar and the future i-Need), ensuring that users receive unique account identifiers.	Operational	Medium	O	Submit documented evidence confirming that access to the customer relationship management application in use in UNMIL (i.e. iNeed) is granted only on the basis of unique credentials and identifiers.	June 2010
29	UNMIL/CITS should undertake periodic tests of its information and communications disaster recovery plan.	Operational	High	O	Submit documented evidence confirming that the plan for periodic tests of the disaster recovery measures has been approved and tests implemented.	August 2010
30	UNMIL/CITS in coordination with representatives of the substantive and support offices should complete the business continuity plan of the Mission with essential information related to "who, how, and where" each functional area will resume and continue their operation in case of a disaster. Upon completion of this task, UNMIL/CITS should update the references to its disaster recovery and business continuity plans by formally referencing two distinct documents, i.e.: a) The "Disaster Recovery Plan"; and b) The "Business Continuity Plan".	Operational	High	O	Submit copy of the approved business continuity plan aligned with the disaster recovery plan of the mission.	Not provided

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

ANNEX 2

*Use this page if the orientation of Annex 2 is portrait. If the orientation is landscape, insert a section break at the end of Annex 1 and continue on the new page. (On the **Insert** menu, point to **Break**, select **Next page** under **Section break types**.) Leave the page blank if not required; do not delete it.*