Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

AUDIT REPORT

ICT governance, security, business continuity and disaster recovery in UNIFIL

UNIFIL needs to strengthen its ICT governance framework with policies and procedures for information security management and ICT operations

26 April 2011
Assignment No. AT2010/672/01

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: Major-General Alberto Asarta Cuevas, Force Commander
A: and Head of Mission
United Nations Interim Force in Lebanon

DATE: 26 April 2011

REFERENCE: IAD: 11-00375

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

SUBJECT:
OBJET: **Assignment No. AT2010/672/01 - Audit of ICT governance, security, business continuity and disaster recovery in UNIFIL**

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 3, 4, 5, 6, 8, 9, 10, 11, and 16 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 12, 13, 14, and 15, and partially accepted recommendation 7. 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 and 14), in its annual report to the General Assembly and semi-annual report to the Secretary-General.

cc: Mr. Choi Soon-hong, Assistant Secretary-General, Chief Information Technology Officer
Mr. Girish Sinha, Director of Mission Support, UNIFIL
Mr. Rudy Sanchez, Director Information Technology Division, DFS
Mr. Anthony O'Mullane, Chief of ICTS, UNIFIL
Mr. Swatantra Goolsarran, Executive Secretary, UN Board of Auditors
Mr. Rohan Wijeratne, Board of Auditors
Ms. Susanne Frueh, Executive Secretary, Joint Inspection Unit
Mr. Mario Baez, Chief, Policy and Oversight Coordination Service, Department of Management
Mr. Byung-Kun Min, Special Assistant to the USG-OIOS
Ms. Eleanor T. Burns, Chief, Peacekeeping Audit Service, OIOS
Mr. Seth Adza, Chief Audit Response Team, DFS
Ms. Amy Wong, Programme Officer, Internal Audit Division, 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, security and business continuity and disaster recovery in the United Nations Interim Force in Lebanon

The Office of Internal Oversight Services (OIOS) conducted an audit of information and communications technology (ICT) governance, security, business continuity and disaster recovery at the United Nations Interim Force in Lebanon (UNIFIL). The overall objective of the audit was to assess the adequacy and effectiveness of internal controls over ICT governance, security management, business continuity and disaster recovery, and to determine compliance with applicable United Nations rules and regulations. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

In general, UNIFIL had deployed a robust ICT infrastructure with a management framework and control environment based on the following control practices:

(a) The user community provided a positive feedback of the services provided by the Information and Communications Technology Services (ICTS) in response to a satisfaction survey conducted in the Mission;

(b) A disaster recovery plan and a backup strategy and procedures were documented. However, as of the time of the audit, a business continuity plan was not documented and tests and validation exercises had not been fully completed;

(c) The Mission developed a service usage policy outlining the requirements for the use of ICT resources. This policy was also complemented by an ICT governance directive identifying data owners of key Mission's applications and access control criteria for granting access to these applications;

(d) ICTS had deployed the server virtualization concept. Approximately 98 per cent of servers had been virtualized. Through this process physical servers were converted into multiple virtual machines for leveraging their processing capability and reducing the number of physical equipment and space in the data centre;

(e) ICTS automated the removal of unnecessary operating system services. Operating system patches were up-to-date and password complexity controls had been enabled on the critical systems;

(f) UNIFIL adopted best practices for the fire suppression systems (FM2000) installed in its data centres; and

(g) UNIFIL had been proactive in the use of green technology by supplementing its energy sources with the use of solar energy.

OIOS also identified some control weaknesses that should be addressed in the area of ICT governance, information security management and operations. In this regard, UNIFIL should:

(a) Document a local ICT strategy and create an ICT steering committee;

(b) Adopt a project management standard and a structured system development life-cycle methodology;

(c) Complement and align disaster recovery procedures with a business continuity plan;

(d) Document service management processes and standard operating procedures for its ICT operations; and

(e) Enhance its information security management by: (i) documenting policies and procedures; (ii) undertaking regular vulnerability assessments; (iii) deploying standard encryption mechanisms; and (iv) strengthening its asset management procedures by documenting and implementing checking in and out procedures.

TABLE OF CONTENTS

I. INTRODUCTION

1. The Office of Internal Oversight Services (OIOS) conducted an audit of information and communications technology (ICT) governance, security, business continuity and disaster recovery in the United Nations Interim Force in Lebanon (UNIFIL). The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

2. UNIFIL was established by Security Council resolutions 425 (1978) and 426 (1978) of 19 March 1978. The most recent extension of the mandate was approved by the Security Council in its resolution 1937 (2010) on 30 August 2010, which extended the mandate of UNIFIL until 31 August 2011.

3. The UNIFIL headquarters is located in Naqoura and houses the offices of the Force Commander, the Director of Mission Support, and the Director of Political and Civil Affairs. Beirut hosts a small UNIFIL Office with liaison and political personnel.

4. The Mission strength as of 30 August 2010 was 11,449 uniformed personnel, including 50 military observers, supported by 315 international civilian personnel and 656 local staff.

5. The annual budget for ICT for the Mission is $24,843,200. The Mission's non-expendable inventory for ICT is currently $39,361,920.

6. A formalized Middle East regional communications and information technology services structure is being proposed for implementation during the 2010/11 period. It is projected that the regionalization initiative would benefit the client base of the four Middle East operations: The United Nations Disengagement Observer Force (UNDOF), UNIFIL, the United Nations Peacekeeping force in Cyprus (UNFICYP) and the United Nations Truce Supervision Organization (UNTSO) which cover 14,655 military contingent personnel, 153 military observers, 69 United Nations police and almost 1,800 civilian staff. The combined budget of the four operations for ICT is $29,948,600 of which 83 per cent is in the UNIFIL ICT budget.

7. Comments made by UNIFIL are shown in *italics*.

II. AUDIT OBJECTIVES

8. The main objective of the audit was to assess the adequacy and effectiveness of controls established in UNIFIL for:

(a) Governing, managing and protecting ICT assets and data;

(b) Defining and assigning ICT roles, responsibilities and reporting lines;

(c) Managing disaster recovery and business continuity operations;

(d) Supporting ICT strategic planning, monitoring, reporting and continuous improvement; and

(e) Managing ICT security, risk assessment and vulnerability testing.

III. AUDIT SCOPE AND METHODOLOGY

9. The audit covered the period 1 January 2009 through November 2010 and included: (a) review of policies, standard operating procedures and guidelines; (b) information provided in response to the audit questionnaires for governance and security; (c) interviews with representatives and staff from substantive areas and the Mission’s support offices; (d) vulnerability tests on selected critical hosts and scans of the Mission’s network; and (e) visits to UNIFIL ICT installations including Sector East headquarters.

IV. AUDIT RESULTS

A. Strategic planning & governance

Local ICT strategy and steering committee

10. The report of the Secretary-General on the budget of UNIFIL for the period from 1 July 2010 to 30 June 2011 outlined a regional information and technology initiative concept for consolidating regional communications and information technology across the Middle East. The expected benefits of this approach are to enable a coordinated delivery of ICT services, avoid duplication of efforts, achieve economies of scale and prevent disparity of services across missions. In this regard, the Department of Field Support (DFS) had documented “The DFS Middle-East Regional ICT service governance model” which outlined the governance framework. However, this new regional consolidation of ICT services was not supported by a documented strategy for its implementation at the Mission level.

11. In addition, ICT operations in UNIFIL were not supported by a strategy describing how the provision of ICT services contributes to and supports the Mission’s mandate and objectives. The absence of an adequate ICT strategic planning process exposes UNIFIL to the risk of: (a) lack of accountability and direction; (b) inability to meet the ICT needs of the Mission; and (c) ICT resources not effectively supporting the Mission.

12. In accordance with the Secretariat’s ICT governance framework a local ICT steering committee should address the ICT needs of the Mission and approve local strategies and plans to ensure: (a) the use of cost effective ICT systems and resources; (b) the adoption of current and future technologies; and (c) monitoring and evaluation of ICT initiatives and projects. UNIFIL had not established an ICT steering committee to serve as a focal point for approving the information needs, priorities and ICT initiatives in the Mission.

Recommendation 1

(1) The UNIFIL Head of Mission should: (a) document a local ICT strategy defining how ICT services will contribute to the achievement of the Mission's objectives; (b) establish an ICT steering committee composed of representatives of key stakeholders in accordance with the ICT governance framework issued by the Office of Information and Communications Technology. The terms of reference of this Committee should include responsibilities for providing direction, control and approval of initiatives, investments and services related to both information management and technology .

13. *UNIFIL accepted recommendation 1, stating that a local ICT strategy will be developed and published through the Head of the Mission based on the United Nations ICT Strategy, UNIFIL Concept of Operations (CONOPS), Force Requirements, Force Commander Compact and Mission Support work plan. It further stated that a UNIFIL ICT Review Committee based on the information package for ICT Governance Structures for Field Missions will be established.* Recommendation 1 remains open pending receipt of a local ICT strategy and evidence of the establishment of the ICT steering committee.

Standard operating procedures

14. ICTS had put in place processes for the provision of services such as network security, server management and application support. However, the majority of ICTS units were operating without standard and documented operating procedures which are needed for providing detailed instructions on ICT operations. The lack of these procedures may lead to inefficiencies and lapses in compliance with policies.

Recommendation 2

(2) The UNIFIL Information and Communications Technology Section should document standard operating procedures for all processes and units in alignment with those established at Headquarters by the Office of Information and Communications Technology and the Department of Field Support. These procedures should be regularly updated for adequacy and relevancy.

15. *UNIFIL accepted recommendation 2, stating that standard operating procedures will be developed over time as this is a major undertaking for a field ICT operation whose standard operating procedures differ radically from those at the Headquarters.* Recommendation 2 remains open pending receipt of documented standard operating procedures.

Information management framework

16. UNIFIL started an information management initiative and established a working group at the beginning of 2010 for documenting an information management framework. However, pending the establishment of this framework, the lack of defined procedures limited the ability of the Mission to manage and control the complete life-cycle of data and information. This condition exposes the Mission to risks related to: (a) the secure collection, distribution and retention of information; (b) unclear roles and responsibilities; (c) lack of operational integration; (d) limited value derived from the information resources available in the Mission; (e) loss of records and unauthorized access to data; and (f) increased storage costs.

17. As part of the information management initiative, UNIFIL requested the Peacekeeping Information Management Unit (PIMU) in New York to undertake an assessment of information management at the Mission. This assessment was completed in July 2010 with the issuance of a report detailing several critical recommendations for facilitating the deployment of an effective information management framework in the Mission. However, as of the time of the audit, these recommendations had not been implemented.

18. UNIFIL indicated that information management is being adequately addressed technically by UNIFIL ICTS in the form of the Intranet/Share Point solution and the electronic Document Management System application. These applications are structured and observe a hierarchical regime in terms of both management and content. Based on the information management framework, UNIFIL took the initiative to request additional staff during budget period 2010/11 for establishing an Information Management Section: however, this requested was not approved. Subsequently, a military staff officer responsible for information management policy has been posted in the Head of Mission’s (HOM) Office and the HOM has issued his directive on information management.

19. OIOS acknowledged the important technical steps taken by ICTS in deploying the Intranet/Share Point solution. Given that the information management initiative is supported by a directive issued by the Head of the Mission, an established working group, a dedicated information management officer and technical tools, OIOS is not issuing additional recommendations at this time. A follow-up will be conducted in due course to review the status of implementation of the initiative and recommendations resulting for the assessment conducted by PIMU/DFS.

Information architecture and data classification

20. 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. This framework also enables the classification of data based on their criticality and sensitivity. UNIFIL had not defined its information

architecture and how the ICT infrastructure and operations will be structured to support the Mission's operations.

21. ST/SGB/2007/6 (Information sensitivity, classification and handling) requires the classification of official data in accordance with three levels of sensitivity and their protection against unauthorized access and disclosure. In the same policy, the Secretary-General provided that sensitive data for reasons of security, safety, privacy and confidentiality should be classified and require special protection.

22. UNIFIL started several initiatives addressing the need for data classification and management which included: (i) a service usage policy outlining the requirements for the use of ICT resources; (ii) a policy directive identifying data owners of key Mission's applications and access control criteria for granting access to these applications; and (iii) an analysis of the usage of broadcasting information and the recent assessment conducted by PIMU of DFS/New York.

23. Since the assessment conducted by PIMU raised relevant recommendations for setting-up a record management system in accordance with the policies of the Secretariat, OIOS is not issuing additional recommendations in this area.

Project management

24. The standard project management methodology adopted by the United Nations Secretariat is "Prince II" (Projects in Controlled Environments). Adhering to a standard project management methodology ensures that key tasks are completed in a logical and controlled order, preventing duplications and rework.

25. ICTS had a dedicated applications development unit and had trained staff members on the use of the "Prince II" methodology. However, this methodology had not been fully reflected in the work practices of ICTS and was not used for key Mission projects. OIOS observed the following weaknesses:

(a) Locally developed applications were not built on the basis of a standard development lifecycle and structured project management methodologies;

(b) There were no formalized processes for users to request the development of new applications and also to provide and approve the business case for new applications; and

(c) In anticipation of the new organization-wide initiatives, such as the Enterprise Resource Planning "UMOJA", Inspira-Talent Management and the enterprise content management, the unit had not conducted an assessment of which locally developed systems will be either replaced by or interfaced with the new enterprise systems.

26. In accordance with the ICT roadmap for field Missions issued by DFS in 2008, requests for the development of new applications had to be reviewed/approved by the local ICT Steering Committee in each Mission on the basis of documented business cases. These business cases should have included minimum information related to requirements for: (i) functions; (ii) disaster recovery and business continuity: (iii) security; and (iv) integration and reporting. Apart from the documentation of functional requirements, other requirements were not documented for the applications developed in UNIFIL.

Recommendation 3

(3) The UNIFIL Information and Communications Technology Section should: (a) formally implement control mechanisms in accordance with the UN standard for project management (Prince-II) for preparing, reviewing, approving and managing ICT projects and initiatives; and (b) in coordination with the Information Communications Technology Division of the Department of Field Support, undertake a comprehensive review of all locally developed applications to determine the need for their future support and maintenance with regard to the planned implementation of the new enterprise applications ERP/UMOJA, Inspira-Talent Management and enterprise content management.

27. *UNIFIL accepted recommendation 3, stating that implementation of the recommendation depends on having an adequate number of staff in the Mission trained on the Prince-II methodology. The second major training will take place in UNIFIL from 28 Feb to 4 March 2011. Upon completion, 14 ICTS staff will be trained on Prince-II. All projects developed after 15 March 2011 will apply this methodology. The list of applications used/supported in UNIFIL is submitted annually to the Information and Communications Technology Division (ICTD) at the New York Headquarters, the last one was submitted on 19 January 2011. This list forms a repository collected from all field Missions against which ICTD/NY assesses requests for new developments. All applications developed in UNIFIL are developed in full coordination with ICTD/NY HQ. UNIFIL is currently in the process of piloting and implementing applications being produced in UNLB under the Field Support Suite (FSS) banner*. Based on UNIFIL’s response, recommendation 3 has been closed.

ICT risk management framework

28. A risk management framework should ensure timely identification and assessment of risks and implementation of corresponding mitigating controls. ICTS did not implement an ICT risk management framework to identify risks and corresponding mitigating controls. The lack of a proper risk assessment and mitigation plan may prevent the Mission from restoring and continuing its activities in case of adverse conditions.

Recommendation 4

(4) The UNIFIL Information and Communications Technology Section should implement an ICT risk management framework and procedures to identify risks and design corresponding mitigating controls.

29. *UNIFIL accepted recommendation 4, stating that ICTS, as with all areas of UNIFIL Mission Support, is included in the Mission's risk matrix which identified nine areas of concern. Risk management in UNIFIL is a Mission initiative and ICTS is fully engaged along with other sections and services.* Based on the action taken by UNIFIL, recommendation 4 has been closed.

B. Asset management

Asset management procedures

30. Effective inventory management should be supported with controls for replenishment, excess items, and tracking the movement and recording of assets. ICTS experienced instances of high stock of some of its expendable line items which resulted in the deployment of surplus stock to other peacekeeping missions. Although the asset management unit operated on the basis of documented procedures, the requisition process and the relationship with the Asset Management Unit (AMU) lacked adequate terms of reference. While the AMU published monthly information about unit stock held in the warehouse, the administration team processing requisitions did not check the availability of unit stock prior to submitting their requests.

Recommendation 5

(5) The UNIFIL Director of Mission Support should implement control mechanisms for ensuring that the requisition of assets is based on the prior verification and confirmation of their availability in the warehouse.

31. *UNIFIL accepted recommendation 5, stating that it has developed and implemented a checklist which includes the verification of the availability of assets in the warehouse and in the strategic deployment stock as well as other important considerations. This checklist is filed with each requisition.* Based on the actions taken by UNIFIL, recommendation 5 has been closed.

Check-in/check-out procedures

32. Effective check-in/check-out procedures should ensure: (a) a documented chain of custody of ICT assets; (b) the termination of users' credentials upon their departure from the Mission; (c) the transfer or archival of relevant official information possessed by the users; and (c) the return of any ICT equipment.

33. UNIFIL had not implemented adequate procedures for managing the check-in/check-out process at the Mission. The process in use did not include individual contractors and was based on different procedures for contingent personnel and civilian staff. OIOS observed the following control weaknesses:

(a) Not all staff members were subject to checking in and out procedures. In some cases staff other than the legitimate user obtained or returned assets on behalf of those not subject to the procedure, creating issues of accountability and ownership for damaged or lost assets;

(b) Staff leaving the Mission were not always visible to the Property Control and Inventory Unit (PCIU) or to ICTS for ensuring the return of assets and the termination of access to systems and applications, preventing the office from being able to reconcile the status of assets allocated to staff; and

(c) The Mission did not have an effective control system for monitoring the status of ICTS assets. In some cases, while users complained about the shortage of personal computers, this equipment was left idle in other offices within the Mission.

Recommendation 6

(6) The UNIFIL Director of Mission Support should review the check-in/check-out procedures to ensure timely and complete account of all assets and credentials allocated to staff members.

34. *UNIFIL accepted recommendation 6, stating that it is implementing the DFS field support suite applications that include the check-in/check-out application being developed in UNLB. International staff will be processed electronically as of 1 April 2011. National staff and staff officers will be included by 30 September 2011.* Based on UNIFIL’s response, recommendation 6 has been closed.

C. Service management

35. ICT services should be managed on the basis of procedures for defining, monitoring and measuring their performance. DFS has adopted the standard service management methodology “Information Technology Infrastructure Library (ITIL)”.

36. UNIFIL implemented some operational processes in line with the ITIL framework with the pilot customer relationship management (CRM) application iNeed. UNIFIL was piloting the first modules of iNeed, which includes service desk and incident management. Related modules covering service performance and capacity management were either under development or will be developed. OIOS is not issuing additional recommendations in this area, pending the results of the pilot iNeed initiative.

Service level agreement

37. Best practices recommend the development of ICT service catalogues documenting the list of standard services provided to the organization, and service level agreements defining expectations, indicators and metrics for measuring performance.

38. Although the user community positively assessed the services provided by ICTS, service level agreement between ICTS and other critical services within the Mission (i.e., Geographical Information Section, Safety and Security, Military Operations) were not documented. The Mission also lacked criteria, standards and performance indicators and metrics for monitoring service delivery and their performance.

39. ICTS could generate a catalogue of its services from the “e-Request” application. However this application did not include details related to roles and responsibilities together with quantitative and qualitative metrics on availability, reliability, performance and capacity.

Recommendation 7

(7) The UNIFIL Information and Communications Technology Section should: (a) document the catalogue of services it provides, together with the criteria, standards and performance indicators for service delivery; and (b) establish internal service level agreements to document and monitor the services provided to the critical functions of the Mission (i.e. Geographical Information Section, Safety and Security, Military Operations).

40. *UNIFIL partly accepted recommendation 7, stating that it accepts only the part of the recommendation regarding the catalogue and not the part including criteria, standard and performance indicators in the catalogue. The catalogue is currently in the process of being updated and will be available by 30 April 2011. The ICTS catalogue of services is currently integrated into the eRequest application. UNIFIL further stated that it will develop ITIL-based service level agreements for critical functions.* OIOS is of the opinion that a catalogue of services without the corresponding criteria, standard and performance indicators for their monitoring and measurement would defeat the purpose of having the catalogue itself. Recommendation 7 remains open pending receipt of the ITIL-based service level agreements developed by UNIFIL with the documentation of the catalogue of services, together with the corresponding criteria, standards and performance indicators.

D. Information security management

Information security requirements

41. The United Nations Secretariat has adopted the information security management standard "ISO 27002". DFS/ICTD has successfully applied this standard in UNLB, Italy. In addition, DFS/ICTD developed a framework of policies for guiding peacekeeping missions through the development and implementation of local policies and procedures in accordance with the standard ISO 27002.

42. One of the main requirements of the standard is that information security activities should be coordinated throughout the organization to ensure consistent application of security policies. In line with this requirement, the DFS vision document "ICTD Roadmap for the Field" indicated that large missions should establish the role of an information security coordinator.

43. ICTS had identified two information security personnel. However, the information security functions of these officers were not clearly defined. Furthermore, they did not have the necessary focus and security training to effectively manage this function.

44. In addition, ICTS had not formalized an information security programme and did not undertake an independent assessment of its information security.

45. There was also no documentation defining formal service level agreement between UNIFIL ICT and the Sector East military contingent concerning the handling of the military's information security requirements.

Recommendation 8

(8) The UNIFIL Head of Mission should: (a) develop and approve an information security policy in accordance with the relevant provisions and standards of the United Nations Secretariat (i.e., ST/SGB/2004/15, ST/SGB/2007/6, ISO 27002); (b) define criteria for the establishment of technical and management security roles; (c) Define the roles and responsibilities of the UNIFIL Information Communications Technology Service and military staff for handling sensitive information and systems; and (d) ensure that the needs for ICT security training are addressed and included in the periodic assessment of the ePAS cycle of staff.

46. *UNIFIL accepted recommendation 8, stating that information security in UNIFIL is based on the ST/SGBs listed in the recommendation and on information sensitivity toolkit version 1 dated 24/02/2010. An information policy officer has been appointed in the office of the Head of the Mission (HOM). An HOM directive is currently being prepared on information management and will be promulgated. The Mission ICTS staff member serving as the security focal point attended training organized by ICTS on "Implementing and auditing*

security controls" in Valencia over the period 12-16 Dec 2010. ICTS will take advantage of upcoming scheduled trainings in this area. This subject will also be included in the ePAS work plan and evaluation. Based on UNIFIL's response, recommendation 8 has been closed.

Information security incident management

47. The professional best practices adopted by the United Nations Secretariat for information security recommend the development and implementation of a formalized incident management program ensuring that: (a) security events are reported through appropriate management channels in a timely manner; (b) all employees, contractors and third party users of information systems and services are required to note and report any observed or suspected security weaknesses in systems or services; (c) management responsibilities and procedures are established to ensure a quick, effective, and orderly response to information security incidents; (d) security threats, weaknesses and incidents are monitored and tests and corrective actions implemented; and (e) an information security awareness programme are employed to increase the level of knowledge and understanding of security requirements among staff.

48. UNIFIL lacked a formalized and documented security incident management process. In addition, periodic vulnerability assessments were not conducted. Without a systematic review and assessment of the vulnerabilities of its network, UNIFIL is unable to identify security threats and control weaknesses, and to timely implement preventive measures to protect the confidentiality of the data and ensure the continuity of the operations.

Recommendation 9

(9) The UNIFIL Information and Communications Technology Section should develop and implement a comprehensive information security incident management process and develop a policy for periodic and independent vulnerability tests of the Mission's network.

49. *UNIFIL accepted recommendation 9, stating that it has developed a network control centre which will include the development and implementation of a comprehensive information security incident management process. Records of any attack on server and network including virus will be logged and managed. UNIFIL also stated that it will invite the Security Officer of ICTD/DFS to perform periodic tests.* Based on the actions taken by UNIFIL, recommendation 9 has been closed.

50. Basic information security awareness was included in the induction briefing of the Mission. The Mission also developed a service usage policy outlining the requirements for the use of ICT resources. This policy was also complemented by an ICT governance directive identifying data owners of key Mission's applications and access control criteria for granting access to these applications. However, UNIFIL lacked an ongoing process to promote continuous awareness of security best practices among the user community.

Recommendation 10

(10) The UNIFIL Director of Administration should develop an information security awareness programme for all staff, using visual aids (i.e., posters) and ongoing awareness training.

51. *UNIFIL accepted recommendation 10 stating that it has received sample posters from ICTD and will launch a campaign by distributing posters and issuing broadcasts on the subject. These campaigns will be periodic.* Based on the action taken by UNIFIL, recommendation 10 has been closed.

<u>Access control management and data integrity</u>

52. The professional best practices adopted by the United Nations Secretariat for information security recommend that users adopt specific criteria for password strengthening to prevent guessing and brute-force attacks.

53. ICTS automated the removal of unnecessary operating system services. Operating system patches were also found to be up-to-date and password complexity controls had been enabled on some critical systems. However, OIOS observed that “guest” and “VIP” accounts established in the Mission did not meet the requirements for password complexity. The logs recording the access of the administrators to the servers were limited to recording only their local access. Access to the servers through the network was not logged, limiting the usefulness of the audit trail of administrator access.

54. Information security procedures and tools should be in place to prevent unauthorized access, misuse of assets, modification and loss of critical data. OIOS observed the following weaknesses associated with these criteria:

(a) UNIFIL did not have a disposal policy for ICT equipment and lacked adequate arrangements for the secure disposal of storage media (hard-drives and other removable media). ICTS relied on re-formatting hard-drives for sanitizing old media. However, this formatting mechanism does not guarantee the complete sanitization of media and the removal of sensitive data or licensed software prior to their transfer of ownership or disposal;

(b) Laptops issued to users handling sensitive data (e.g., Security Section) were not being encrypted. This condition could expose UNIFIL data to risks of unauthorized access or loss of confidentiality and integrity; and

(c) ICTS had deployed a tool (websense) for Internet filtering. However, ICTS had not defined, in consultation with the other sections, the criteria for Internet filtering. These criteria should have included rules, categories of users and nature of website for granting access and/or exceptions.

Recommendations 11 to 13

(11) The UNIFIL Information and Communications Technology Service should design and implement procedures for ensuring that access control management is supported by: (a) criteria for password strengthening are employed for all account types (including "Guest" and "VIP" accounts); and (b) audit logs recording user activities regardless of their method of access, with information about exceptions and information security events.

(12) The UNIFIL Director of Administration should: (a) document an ICT asset disposal policy; (b) adopt data sanitizing techniques to permanently delete data from storage media and devices prior to their transfer or disposal; and (c) define and configure more stringent security measures for laptops used for processing sensitive information (e.g., encryption of laptop hard-drive and removable media).

(13) The UNIFIL Head of Mission should develop, in consultation with relevant stakeholders, an Internet filtering policy defining standard rules, categories of users and nature of websites for granting access and/or exceptions.

55. *UNIFIL accepted recommendation 11 and stated that it has implemented procedures using group policy for ensuring access control.* Based on the action taken by UNIFIL, recommendation 11 has been closed.

56. *UNIFIL did not accept recommendation 12, stating that it strictly follows the property management manual and all HQ directives with regard to property management including disposal relating to ICT assets. The recommendation requires a global approach as there is no HQ policy currently authorizing these changes. Data stored on UNIFIL laptops is of a routine nature. In the absence of HQ guidance in case of exceptions, these will be dealt with by the client addressing the request in writing and the case will be dealt with on an ad hoc basis*. OIOS is unable to accept the explanation provided by UNIFIL with regard to the sanitization of removable media because they are not in line with the policies published at the United Nations Headquarters and available on the United Nations' intranet (http://iseek.un.org/LibraryDocuments/1637-201101071558085748836.pdf). OISO reiterates recommendation 12 that remains open pending receipt of evidence demonstrating that UNIFIL has: (i) developed and implemented a local ICT asset disposal policy; (ii) adopted media sanitization techniques; and (iii) implemented security measures for laptops used to process sensitive information.

57. *UNIFIL did not accept recommendation 13 stating that the general policy for web filtering is published. Exceptions to this policy are dealt with through an eRequest, approved by the requestor's Chief of Section/Branch and*

the ICTS Chief. Additional access is approved based strictly on work requirements and on the capacity of the system to handle the additional load. The work requirement is certified by the relevant Section or Branch Chief and the capacity is certified by the ICTS Chief. The key approvers are involved in the process. OIOS did not receive, during the course of the audit, copy of the web filtering policy mentioned by UNIFIL in its response. Therefore, recommendation 13 remains open pending receipt of the published web filtering policy.

Secure distribution of code cables

58. The use of code cables (encrypted fax) should ensure the confidentiality, authenticity and integrity of sensitive/confidential information.

59. Code cables were subject to continuous movement between various offices within the Mission and in some instances had been distributed to as many as thirty officials. This condition resulted in the production of multiple copies and several internal distributions with limited oversight and control of the documents, thus exposing them to the risk of unauthorized access.

60. UNIFIL indicated that:

(i) The distribution of code cables is determined by the Head of Mission and is issued as a written directive;

(ii) His decision is executed by the concerned parties;

(iii) ICTS adheres fully to the Head of Mission’s decision and to the policies outlined in the information sensitivity toolkit;

(iv) The Communications Centre adheres strictly to all related directives on retention of classified documents; and

(v) The information sensitivity toolkit is widely published and available throughout the Mission and defines retention policy for all classified documentation handled and archived by the communications centre.

61. Since the assessment conducted by PIMU raised relevant recommendations for setting up a record management system in accordance with the policies of the Secretariat, OIOS is not issuing additional recommendations in this area.

Encrypted communications

62. ST/SGB/2007/6 (Information sensitivity, classification and handling) specifies that “the Heads of departments or offices shall ensure that minimal standards are maintained in the handling of classified information received by or originating from their department or office including that the electronic

transmission of classified information shall be performed only through the use of protected means of communications."

63. UNIFIL had not addressed the requirements established in ST/SGB/2007/6 for the classification of information and their electronic transmission using protected means of communications. In addition, the results of OIOS interviews and review of information systems in UNIFIL highlighted the need for a systematic review of the needs for the deployment and support of encrypted communications. In particular, the military component expressed a need for sufficient encrypted hardware to secure classified documents generated during the course of their operations.

Recommendation 14

(14) The UNIFIL Head of Mission should, in coordination with the Office of Information and Communications Technology and the Information and Communications Technology Division of the Department of Field Support, establish standard techniques and procedures for the deployment of encryption in the Mission in line with the requests of the military component.

64. *UNIFIL did not accept recommendation 14, stating that ICTS has deployed the standard suite of encrypted systems in use by peacekeeping missions. These include the Secretary-General's encrypted voice/data network and the secured DFS VTC network. Additional UNIFIL specific requirements for encrypted systems have been effectively dealt with through joint working groups between Military and Mission Support in consultation with ICTD/NY. These additional UNIFIL specific encrypted systems include a secure internet protocol (IP) data network, an encrypted VHF radio network and an electronic counter measures system. UNIFIL has in addition a suite of encrypted options including a specific encrypted telephone network for security, an encrypted mobile phone system and secure desktop for video/teleconference (VTC).*

65. OIOS requested UNIFIL to provide evidence demonstrating that the specific requirements for encrypted systems have been effectively dealt with through joint working groups between Military and Mission Support. UNIFIL provided a draft memo, with incomplete information and date (July 2009), related to a proposal for the establishment of VHF encrypted communication system. OIOS is of the opinion that given the draft nature of the memo, its incomplete content and limited scope (radio), this evidence does not demonstrate that the issues pertaining to recommendation 14 have been adequately addressed. Therefore, OIOS reiterates recommendation 14 that remains open pending receipt of evidence demonstrating that UNIFIL has established standard techniques and procedures for encrypted systems in the Mission addressing the requirements of the military component.

Business continuity and disaster recovery

66. Business continuity planning allows an organization to prepare for disruptive events. The plan should also include a disaster recovery component, which is a technology enabled process for ensuring the recovery and restoration of critical ICT operations and data.

67. ICTS had documented a disaster recovery plan to ensure the retention and recovery of critical data. However, the Mission had not documented a business continuity plan in line with its disaster recovery plan. While this condition would allow the Mission to ensure the recovery of ICT assets and data in the event of a disaster, it would limit its ability to preserve and restore the information for ensuring the continuation of critical business processes as the data and ICT systems are of no value if there are no business criteria and plans for their use in case of emergency.

68. In addition to the risks identified above, OIOS also observed that:

(a) Staff located in the sectors were not familiar with the disaster recovery plan and were unsure of what to do should the plan be activated;

(b) Although the disaster recovery plan contained provisions for its periodic test (twice a year), and UNIFIL had scheduled and conducted some tests, not all testing scenarios had been performed as planned;

(c) The availability of power was perceived as a critical risk to the Mission. However, ICTS had not included this threat in its disaster recovery planning scenario even though UNIFIL had been proactive in the use of green technology by supplementing its energy sources with the use of solar energy; and

(d) ICTS had documented a backup strategy and procedures based on full and incremental schedules. All data stored on the UNIFIL ICTS network was backed up daily to UNLB in accordance with the DFS standard retention policy and the local policy issued by Mission Support. However, the Mission had not undertaken an exercise to identify critical applications and data, and whether the defined retention period of 30 days was adequate for all functions.

Recommendation 15

(15) The UNIFIL Head of Mission should ensure the completion of the following tasks: (a) identification of the Mission’s critical applications; (b) conduct a business impact assessment and document a business continuity plan integrated with the disaster recovery plan; (c) design and implement procedures for ensuring that the disaster

recovery plan is known by all staff of the Mission; (d) define disaster recovery scenarios that include power failure; (e) conduct periodic tests of the recovery plan; and (f) complement its backup strategy with the identification of critical applications and data, and confirm whether the 30 days retention period is adequate for all functions.

69. *UNIFIL did not accept parts (a), (b) and (c) of recommendation 15, stating that the recommendations do not take into consideration the current ICTD/NY policy of the daily backup of all data stored on its field Mission networks to the United Nations Logistic Base (UNLB) in Brindisi. UNIFIL ICTS has a documented disaster recovery and business continuity plan which was fully tested during the war in Lebanon in 2006 and was subsequently updated.* OIOS is unable to accept the explanations provided by UNIFIL because they did not address the recommendation. The UNIFIL disaster recovery plan version 3.0 stated that the plan should be tested at least twice a year. UNIFIL's response to recommendation 15 indicated that the effectiveness of the plan was demonstrated during the war in Lebanon in 2006. Furthermore, the plan did not contain a list of Mission's critical applications, business impact analysis and a continuity plan integrated with the disaster recovery plan. Therefore, OIOS reiterates parts (a), (b) and (c) of recommendation 15 that remain open pending receipt of: (i) a business impact analysis; (ii) a disaster recovery plan integrated with a business continuity plan; and (iii) a communication initiative to create awareness about the disaster recovery and business continuity plan.

70. *UNIFIL accepted parts (d), (e) and (f) of recommendation 15, stating that it has a fully documented business continuity plan which was successfully tested in 2006 with the establishment of the UNIFIL parallel administration in the United Nations Peacekeeping Force in Cyprus (UNFICYP) and that all data sitting on UNIFIL's data network is included in its backup schedules. All data is copied daily to UNLB where DFS retention policies are applied. Recovery scenario and periodic tests are included in the disaster recovery and business continuity document. A circular will be issued concerning the disaster recovery plan.* OIOS reviewed the UNIFIL disaster recovery plan version 3.0, dated April 2010. This plan did not include: (i) evidence of periodic tests (twice a year as required by the plan); (ii) disaster recovery scenarios including power failures; and (iii) training plans. Parts (d), (e) and (f) of recommendation 15 remain open pending receipt of documentation demonstrating that the requirements listed in 15 (d) to (f) have been addressed.

Physical and environmental security of ICT resources and assets

71. The professional best practices adopted by the United Nations Secretariat recommend the design and implementation of physical protection against damage from fire, flood, earthquake, explosion, civil unrest and other forms of natural or man-made disasters. UNIFIL had adopted best practices for the use of green technologies and the fire suppression systems (FM2000) installed in its HQ data centres.

72. However, UNIFIL 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, as detailed in Annex 2.

73. OIOS also observed that the responsibility for monitoring, retaining and accessing the closed-circuit television (CCTV) tapes of ICTS locations was not clearly defined and that the Mission did not have a retention policy for these tapes. Furthermore, OIOS was informed that a safe located in the main data centre contained old tapes. However, UNIFIL staff was not aware of the specific content of neither the safe nor its sensitivity, and the access code for opening the safe was unknown.

74. These control weaknesses could result in the loss of data confidentiality, integrity and availability of critical UNIFIL information assets.

Recommendation 16

(16) The UNIFIL Information and Communications Technology Section should: (a) strengthen the current physical security controls of the data centres in Sector East by installing closed-circuit television (CCTV) cameras, fire extinguishers and climate monitoring tools in all data centres; (b) allocate the responsibility for monitoring, retaining and granting access to the CCTV tapes of ICTS locations; and (c) investigate the contents of the safe in the main data centre and apply the United Nations retention and archiving policies to the safe's contents.

75. *UNIFIL accepted recommendation 16, stating that it has strengthened the physical control by placing iron steps at the 8-33 ICTS shelter door. This is the only elevated shelter in the area of operations. Also, fire extinguishers have been installed and instead of closed circuit cameras (CCTV), it will install a swipe card access control system in all ICT shelters. UNIFIL will develop and promulgate a standard operating procedure on access to CCTV tapes and a new safe will be available in March, and the contents will be catalogued and moved from existing storage.* Based on the actions taken by UNIFIL, recommendation 16 has been closed.

V. ACKNOWLEDGEMENT

76. We wish to express our appreciation to the Management and staff of UNIFIL 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 UNIFIL Head of Mission should: (a) document a local ICT strategy defining how ICT services will contribute to the achievement of the Mission's objectives; (b) establish an ICT steering committee composed of representatives of key stakeholders in accordance with the ICT governance framework issued by the Office of Information and Communications Technology. The terms of reference of this Committee should include responsibilities for providing direction, control and approval of initiatives, investments and services related to both information management and technology.	Governance	High	O	Submit copy of the local OCT strategy and evidence of the establishment of the ICT governance structures.	30 April 2011
2.	The UNIFIL Information and Communications Technology Section should document standard operating procedures for all processes and units in alignment with those established at Headquarters by the Office of Information and Communications Technology and the Department of Field Support. These procedures should be regularly updated for adequacy and relevancy.	Governance	Medium	O	Document standard operating procedures.	31 December 2011
3.	The UNIFIL Information and Communications Technology Section should: (a) formally adopt and implement control mechanisms in	Governance	Medium	C		Implemented

Recom. no.	Recommendation	Risk category	Risk rating	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
	accordance with the UN standard for project management (Prince-II) for preparing, reviewing, approving, and managing ICT projects and initiatives; and (b) in coordination with the Information Communications Technology Division of the Department of Field Support, undertake a comprehensive review of all locally developed applications to determine the need for their future support and maintenance with regard to the planned implementation of the new enterprise applications ERP/UMOJA, Inspira-Talent Management and enterprise content management.					
4.	The UNIFIL Information and Communications Technology Section should implement an ICT risk management framework and procedures to identify risks and design corresponding mitigating controls.	Governance	Medium	C		Implemented
5.	The UNIFIL Director of Mission Support should implement control mechanisms for ensuring that the requisition of assets is based on the prior verification and confirmation of their availability in the warehouse.	Operational	Medium	C		Implemented
6.	The UNIFIL Director of Mission Support should review the check-in/check-out procedures to ensure timely and complete account of all assets and credentials allocated to staff members	Operational	Medium	C		Implemented

Recom. no.	Recommendation	Risk category	Risk rating	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
7.	The UNIFIL Information and Communications Technology Section should: (a) document the catalogue of services it provides, together with the criteria, standards and performance indicators for service delivery; and (b) establish internal service level agreements to document and monitor the services provided to the critical functions of the Mission (i.e., Geographical Information Section, Safety and Security, Military Operations).	Governance	Medium	O	Document the catalogue of services, together with the criteria, standards and performance indicators for service provision.	Not provided
8.	The UNIFIL Head of Mission should: (a) develop and approve an information security policy in accordance with the relevant provisions and standards of the United Nations Secretariat (i.e., ST/SGB/2004/15, ST/SGB/2007/6, ISO 27002); (b) define criteria for the establishment of technical and management security roles; (c) define the roles and responsibilities of the UNIFIL Information Communications Technology Service and military staff for handling sensitive information and systems; and (d) ensure that the needs for ICT security training are addressed and included in the periodic assessment of the ePAS cycle of staff.	Governance	Medium	C		Implemented
9.	The UNIFIL Information and Communications Technology Section should develop and implement a comprehensive information security incident management process and develop a policy for periodic and independent vulnerability tests of the Mission’s network.	Operational	Medium	C		Implemented

Recom. no.	Recommendation	Risk category	Risk rating	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
10.	The UNIFIL Director of Administration should develop an information security awareness programme for all staff, using visual aids (i.e., posters) and ongoing awareness training	Information resources	Medium	C		Implemented
11.	The UNIFIL Information and Communications Technology Section should design and implement procedures for ensuring that access control management is supported by: (a) criteria for password strengthening are employed for all account types (including "Guest" and "VIP" accounts); and (b) audit logs recording user activities regardless of their method of access, with information about exceptions and information security events	Operational	Medium	C		Implemented
12.	The UNIFIL Director of Administration should: (a) document an ICT asset disposal policy; (b) adopt data sanitizing techniques to permanently delete data from storage media and devices prior to their transfer or disposal; and (c) define and configure more stringent security measures for laptops used for processing sensitive information (e.g., encryption of laptop hard-drive and removable media).	Governance	Medium	O	Document a local ICT asset disposal policy, adopt media sanitization techniques; and implement of security measures for laptops used to process sensitive information.	20 February 2011
13.	The UNIFIL Head of Mission should develop, in consultation with relevant stakeholders, an Internet filtering policy defining standard rules, categories of users and nature of websites for granting access and/or exceptions.	Operational	Medium	C	Provide copy of the Internet filtering policy.	Implemented
14.	The UNIFIL Head of Mission should, in coordination with the Office of Information and Communications Technology and the Information and	Operational	High	O	Submit documented evidence demonstrating that UNIFIL has established standard techniques and procedures for encrypted systems in the Mission addressing the	Not provided

Recom. no.	Recommendation	Risk category	Risk rating	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
	Communications Technology Division of the Department of Field Support, establish standard techniques and procedures for the deployment of encryption in the Mission in line with the requests of the military component.				requirements of the Military component.	
15.	The UNIFIL Head of Mission should ensure the completion of the following tasks: (a) identification of the Mission's critical applications; (b) conduct a business impact assessment and a business continuity plan integrated with the disaster recovery plan; (c) design and implement procedures for ensuring that the disaster recovery plan is known by all staff of the Mission; (d) define disaster recovery scenarios that include power failure; (e) conduct periodic tests of the recovery plan; and (f) complement its backup strategy with the identification of critical applications and data, and confirm whether the 30 days retention period is adequate for all functions.	Governance	Medium	O	Submit documented evidence demonstrating that UNIFIL has: a) Identified the Mission's critical applications; b) Completed a business impact assessment and integrated a business continuity plan with the disaster recovery plan; (c) Ensured adequate awareness of the business continuity and disaster recovery plan across the Mission; (d) Designed disaster recovery scenarios that include power failure; (f) Conducted the required of the plan twice a year; and (g) Complemented its backup strategy with the identification of critical applications and data, and confirmed that the 30 day retention period is adequate for all functions.	Not provided
16.	The UNIFIL Information and Communications Technology Section should: (a) strengthen the current physical	Operational	Medium	C		Implemented

Recom. no.	Recommendation	Risk category	Risk rating	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
	security controls of the data centres in Sector East by installing closed-circuit television (CCTV) cameras, fire extinguishers and climate monitoring tools in both data centres; (b) allocate the responsibility for monitoring, retaining and granting access to the CCTV tapes of ICTS locations; and (c) investigate the contents of the safe in the main data centre and apply the United Nations retention and archiving policies to the safe's contents.					

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

ANNEX 2

Physical and environmental security of ICT resources and assets
List of control gaps

Location	Gaps
Sector east H-33 server	➢ No fire extinguisher; ➢ No camera for monitoring; ➢ No climate control tool to monitor changes in climatic conditions within the container; ➢ No smoke detector; and ➢ No steps for ease of access into the DC had to jump in and out.
Sector east HQ server room	➢ No camera for monitoring; and ➢ No climate control tool to monitor changes in climatic conditions within the container.