



INTERNAL AUDIT DIVISION

AUDIT REPORT

ICT governance, strategic management, and security at the United Nations Mission to the Democratic Republic of Congo (MONUC)

Missing controls in the mechanisms in place for governance, strategic management, and security of ICT put the system at risk of ineffectiveness.

**31 December 2008
Assignment No. AT2008/620/01**

United Nations  Nations Unies

INTEROFFICE MEMORANDUM

MEMORANDUM INTERIEUR

OFFICE OF INTERNAL OVERSIGHT SERVICES BUREAU DES SERVICES DE CONTRÔLE INTERNE
INTERNAL AUDIT DIVISION DIVISION DE L'AUDIT INTERNE

TO Mr. Alan Doss, Special Representative of the Secretary-
A General
United Nations Mission to the Democratic Republic of
Congo (MONUC)

DATE 31 December 2008

for
FROM Dagfinn Knutsen, Director
DE Internal Audit Division, OIOS
Fatung

REFERENCE IAD: 08-02075

SUBJECT **Assignment No. AT2008/620/01 - Audit of ICT governance, strategic management, and security**
OBJET **at the United Nations Mission to the Democratic Republic of Congo (MONUC).**

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 15, 16, 17, 19, 20 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 4, 5, 6, 9 and 25. 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 18 and 21), in its annual report to the General Assembly and semi-annual report to the Secretary-General.

cc: Mr. Hany Abdel-Aziz, Director of Mission Support, MONUC
Mr. Gilles Briere, Chief, Integrated Support Services, MONUC
Mr. Laurence Minguell, Officer in Charge, Communication and Information Technology Section, MONUC
Mr. Swatantra Goolsarran, Executive Secretary, UN Board of Auditors
Ms. Maria Gomez Troncoso, Officer-in-Charge, Joint Inspection Unit Secretariat
Mr. Moses Bamuwanye, Chief, Oversight Support Unit, Department of Management
Mr. Byung-Kun Min, Programme Officer, 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:

Dagfinn Knutsen, Tel: +1.212.963.5650, Fax: +1.212.963.2185,
e-mail: knutsen2@un.org

DEPUTY DIRECTOR:

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

CHIEF PEACEKEEPING AUDIT SERVICE:

Eleanor Burns: Tel: +1.917.367.2792, Fax: +1.212.963.3388,
e-mail: burnse@un.org

EXECUTIVE SUMMARY

ICT governance, strategic management, and security of the United Nations Mission to the Democratic Republic of Congo (MONUC)

OIOS conducted an audit of information, communication & technology (ICT) governance, strategic management, and security of the United Nations Mission to the Democratic Republic of Congo (MONUC). The overall objective of the audit was to ensure that ICT governance, strategic management, and security within MONUC was adequate and effective. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

In general the framework for ensuring effective ICT governance, strategic management, and security was in place. For instance, responsibility for ICT was defined and well documented. The ICT capabilities to support the Mission's requirements were also defined and generally, the ICT management and control environment were aligned with MONUC's key risks. However, some of the constituent parts of an effective governance, strategic management, and security processes have not been implemented, as summarised below:

- a) ICT related standard operating procedures (SOPs), administrative instructions (AIs), and other policies and procedures were not uniformly disseminated at MONUC, thus impacting their application;
- b) There was no evidence that the following existed for end user application development:
 - i) Standards;
 - ii) Management and control processes; and
 - iii) Appropriate development tools.
- c) There were no mechanisms in place to ensure adequate consideration of the impact that UN wide ICT initiatives/projects may have on the Mission's ICT operational working plan. Relevant UN-wide ICT initiatives/projects are represented by the new Enterprise Resources Planning (ERP), Customer Relationship Management (CRM), and Enterprise Content Management (ECM) initiatives;
- d) There was no process in place whereby applications developed to address local ICT requirements, could be sourced from other Missions that may have developed similar solutions;
- e) On occasions, separation of duties was by-passed due to staffing limitations. Staff were sometimes required to multi-task in order to cover essential or business critical services;
- f) There was a limitation to the operational effectiveness of the staffing structure in that, for example, technical field staff did not report to

Communication, Information Technology Service (CITS) but to the Regional Management. This created a situation whereby CITS management had no direct line management responsibility for field technicians;

- g) MONUC has not established an ICT committee, to ensure that ICT goals and requirements were discussed and decided upon at the appropriate management level;
- h) UN-wide initiatives/projects that may have an impact on the Mission, such as the ERP, CRM and ECM initiatives, were not considered during the work planning process;
- i) The ICT performance and capacity plan has not been fully formalised into a process for developing, reviewing and adjusting performance and infrastructure capacity;
- j) The Mission's network was subject to near capacity bandwidth utilisation; and
- k) There was no evidence that a comprehensive Mission-wide business impact assessment for disaster recovery purposes had been undertaken.

TABLE OF CONTENTS

Chapter	Paragraphs
I. INTRODUCTION	1-4
II. AUDIT OBJECTIVES	5
III. AUDIT SCOPE AND METHODOLOGY	6-7
IV. AUDIT FINDINGS AND RECOMMENDATIONS	
A. Governance	8-32
B. Strategic management	33-41
C. Security	42-67
V. ACKNOWLEDGEMENT	68
ANNEX 1 – Status of Audit Recommendations	

I. INTRODUCTION

1. The Office of Internal Oversight Services (OIOS) conducted an audit of information, communication & technology (ICT) governance, strategic management, and security of the United Nations Mission to the Democratic Republic of Congo (MONUC). The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.
2. MONUC has the UN peacekeeping operations' largest ICT network. The active directory infrastructure comprises of approximately 5,719 users, 4,838 computer accounts and 24 domain controllers.
3. The approved resources for MONUC for the period from 1 July 2007 to 30 June 2008 are \$1,115,654,300, including \$32,865,200 for communications and \$8,247,300 for information technology (source: A/61/767). Compared with approved resources for the period 1 July 2006 to 30 June 2007, communications resources increased by 14.1 percent and information technology increased by 10 percent. There has been no significant investment growth in these two areas during the current budget cycle.
4. Comments made by The MONUC Office/Mission Support are shown in *italics*.

II. AUDIT OBJECTIVES

5. The main objectives of the audit were to determine whether:
 - (a) A system is in place for the governance of ICT resources;
 - (b) Adequate policies and procedures are in place for ICT strategic planning and management; and
 - (c) Clear roles and responsibilities are defined for ICT operations and security.

III. AUDIT SCOPE AND METHODOLOGY

6. The audit covered the current ICT structure and processes of MONUC headquarters in Kinshasa, which reflected those of other MONUC locations. The audit focused on:
 - a) ICT governance, strategic planning, project and performance management;
 - b) ICT project management;
 - c) Management of ICT assets;
 - d) Network management and security;
 - e) Disaster recovery and continuity management; and
 - f) Physical and environmental security.
-

7. Interviews were held with key officers who held responsibilities for ICT processes and assets. Documentation was obtained and reviewed to ascertain the ICT governance structure, strategic management and security environment. Tests were undertaken to confirm the adequacy of controls and to identify threats, risks and vulnerabilities that may affect the ICT control environment.

IV. AUDIT FINDINGS AND RECOMMENDATIONS

A. Governance

MONUC ICT policies and procedures insufficiently communicated

8. Instructions and guidelines that reflect MONUC ICT policies and procedures should be disseminated to all concerned Mission personnel and maintained as a complete library. OIOS found, however, that ICT related standard operating procedures (SOPs), administrative instructions (AIs), and other policies and procedures were not uniformly known at MONUC, thus impacting their application. Furthermore, SOPs for ICT project management and help desk operations were not systematically documented. In some cases, policies and procedures existed but were not updated. Several policies and procedures were still labeled as “draft” several years after their issuance. These gaps have resulted in functional areas creating their own procedures, without this process being systematically documented and approved by MONUC management. An example of this condition was represented by the “Mail, Pouch and Reproduction Training and Reference Manual” compiled by the supervisor of the unit. Inadequate or incomplete documentation of policies and procedures could create risks of misinterpretation or non-compliance, and also negatively affect monitoring and oversight of MONUC compliance with ICT policies and procedures.

Recommendation 1

(1) The MONUC Office of Mission Support should review and update the current library of ICT policies and procedures for adequacy and relevance, and proceed to document policies and procedures where gaps have been identified. In addition, a formal process should be put in place to ensure the continuous update of ICT policies and procedures.

9. *The MONUC Office of Mission Support accepted recommendation 1 and stated that policies and standard operating procedures are currently under review by the management of the Mission and will be released as cleared. Recommendation 1 remains open pending full review and update of the current library of ICT policies and procedures.*

Lack of a framework for end user application development

10. There was no evidence that the following existed for end user application development:

- a) Standards;
- b) Management and control processes; and
- c) Appropriate development tools.

MONUC administrative instruction titled “SOP CITS SOP\AI on System Development” issued in March 2008 attempted to address the requirements for a structured and consistent approach for project management. However, the instruction is a one page summary document, insufficiently detailed to represent a framework for project management. Without adequately documented procedures and guidelines, MONUC faces the risks that ICT projects do not meet requirements, thus creating delays, rework, increased costs, and potential interoperability and integration problems.

Recommendation 2

(2) The MONUC Office of Mission Support should document a detailed project management framework to include standards for end user development, management and appropriate development tools.

11. *The MONUC Office of Mission Support accepted recommendation 2 and stated that MONUC adhered to the project management methodologies “PRINCE2” and “PMI Project Management framework”. Recommendation 2 remains open pending receipt of documented evidence of the project management procedures issued in accordance with the frameworks adopted by the Mission, along with the defined standards for end user development.*

12. According to ST/SGB/2003/17, the UNHQ established decision-making body dealing with high level business cases (HLBC) is the ICT board, which reviews projects in excess of \$200,000. Section 4.4 of the ST/SGB/2003/17 requires that local committees be set up to “*maintain and update information on departmental systems; resources and assets; existing systems to confirm their cost effectiveness; and ensure that standard methodologies are consistently used for information and communication technology projects*”. OIOS was informed that projects at MONUC were prioritised based on the Mission’s operational requirements, and that this function was performed by the Mission Support Centre (MSC). However, the terms of reference and mandate of the MSC are not in line with the criteria established in ST/SGB/2003/17. Therefore, MONUC is exposed to the risk of an ineffective decision making process without a dedicated ICT committee.

Recommendation 3

(3) The MONUC Office of Mission Support should establish a local ICT committee in line with ST/SGB/2003/17, to maintain and

update information on departmental systems, resources and assets, and existing systems; to confirm the cost effectiveness of information systems; and ensure that standard methodologies are consistently used for information and communication technology projects.

13. *The MONUC Office of Mission Support accepted recommendation 3 and stated that a local ICT committee will be established.* Recommendation 3 remains open pending establishment of a local ICT committee, and related terms of reference for the review of departmental systems, projects, and their cost effectiveness.

14. The Mission uses the change management process as the framework for ensuring that new developments and changes to existing systems are managed and controlled. However, the document presented to OIOS as the procedural guideline on change management was found to be insufficient. For instance, there were no details as to what systems development methodology was appropriate for different project sizes. It was also not evident that the various stages of the development life cycle, such as testing and validation against requirements, were in operation. The lack of guidelines in this area could result in the use of inconsistent and inadequate tools for project management and system development, which could lead to unclear responsibilities within projects; and development and implementation errors which could cause delays and lead to increased costs.

15. Forty three 'in-house' developed applications were identified, some of which appeared to have been critical to the effectiveness of MONUC administrative processes. An example of this was the telephone billing system, an online billing system used to monitor and administer telephone usage across the Mission. However, there was no evidence that an assessment had been undertaken to determine whether these applications will be replaced by, or integrated with new UN ICT initiatives, such as Enterprise Resources Planning (ERP), Customer Relationship Management (CRM) and Enterprise Content Management (ECM). The consequences of not reviewing the development of in-house applications could lead to duplication of efforts, and interoperability and integration problems.

Recommendations 4 and 5

The MONUC Office of Mission Support should:

(4) Undertake a review of all current in house developed systems and determine whether they will be integrated into the new Enterprise Resource Planning, Customer Relationship Management, and Enterprise Content Management initiatives.

(5) Document a procedure to ensure that before any future development of a system application, an assessment should be undertaken to verify that the same functionality would not be provided by the Enterprise Resource Planning, Customer

Relationship Management, and Enterprise Content Management initiatives, being undertaken at the Secretariat.

16. *The MONUC Office of Mission Support did not accept recommendation 4 and 5, and stated that integration with the UN ICT initiatives (ERP, CRM and ECM) is not under the purview of any mission, as these are managed at UNHQ.* In the opinion of OIOS, MONUC is also responsible for ensuring efficient integration of its systems with the new UN ICT initiatives, and prevent duplication. OIOS therefore reiterates recommendations 4 and 5, which remains open pending an assessment of these systems.

17. There was no process in place to allow sourcing of local ICT solutions from other Missions, to reduce the need to develop local applications to aid business requirements, and mitigate duplication, waste and inefficiency risks.

18. OIOS requested documentation to confirm the testing of new developments or enhancements. However, no documentation was provided for the testing of recently developed systems such as the development of the web version of the Cargo Movement Request system (E-CMR). OIOS was provided with examples of project sign off sheets. OIOS noted that these documents provided for the business user sign off of developments that have been adequately completed and tested. However, the project sign off sheets did not provide evidence of a formal testing process. In addition, some pending high risk issues were annotated on these documents, but there was no evidence of a follow-up process or checks to confirm resolution of outstanding issues before sign off. This could result in implementation of systems that do not meet specifications and their inability to connect or interface with other key business systems.

Recommendation 6

(6) The MONUC Office of Mission Support should establish a process whereby the ICT requirements of Mission sites can be met through integrated working practices or sharing of local developments between different Missions, to prevent duplication, waste and inefficiencies.

19. *The MONUC Office of Mission Support did not accept recommendation 6 and stated that UNHQ-Department of Peacekeeping Operations has already established that all Mission CITS should refer to centralized E-portal prior to performing any development work.* In the opinion of OIOS, the creation of a centralized E-portal is a relevant step in the establishment of a shared repository of working practices. However, to ensure the effectiveness of the system, and prevent duplications, the creation of an E-portal must be supported by a clear process instructing the missions when and how to consult the portal to adopt the shared working practices. Therefore, recommendation 6 remains open pending receipt of documented evidence regarding the process established by UNHQ-DPKO for the use of the centralized E-portal, and the integration and sharing of working practices between Missions.

Separation of duties by-passed due to staffing shortages

20. Separation of duties existed to provide for the secure use of ICT facilities among the main ICT functions of management, support, development and operations. In addition, controls were in place to ensure that officers were not allowed conflicting duties on business critical systems. However, it was noted that due to staffing limitations, on several occasions staff were required to multi-task in order to cover essential or business critical services. For instance, OIOS was informed that in some sector field offices, technical staff also performed asset management duties. Even though there were some controls to mitigate against the risks posed by the lack of segregation, OIOS deemed the controls inadequate. For instance, restrictions were placed on the amount of assets that the technical staff was allowed to hold. This mitigating control did not prevent loss of asset but reduced exposure to loss.

Recommendation 7

(7) The MONUC Office of Mission Support should ensure that ICT duties are adequately segregated.

21. *The MONUC Office of Mission Support accepted recommendation 7 and stated that in order to prevent multi-tasking across ICT fields, additional staff is required. 10 posts were approved in budget 2008-09 for which recruitment is ongoing. Recommendation 7 remains open pending receipt of evidence documenting that MONUC ICT duties have been adequately segregated.*

Misalignment in the ICT reporting line structure

22. OIOS reviewed the Mission's staffing structure and noted that responsibility for ICT was defined, and there was an officer, the Chief Communication, Information Technology Services (CCITS) responsible for overseeing adherence to policies, procedures and controlling the ICT investment. However, there was a limitation to the operational effectiveness of this structure in that, technical field staff did not report to CITS but to the Regional Management. This created a situation whereby CITS management had no direct line management responsibility for field technicians, but instead was only responsible for day to day 'technical' supervision of their work. The risks associated with this structure are:

- a) Uncoordinated approach to the ICT strategies;
- b) Mismatch between the ICT functional strategies at the regional and Mission level;
- c) Lack of a controlled and secure environment;
- d) Confusion amongst staff regarding reporting lines;
- e) Potential conflicts between the ICT functions performed by CITS/Kinshasa and the Regional Management, as to what their staffing requirements are;
- f) Training requirements going undetected; and
- d) Mission critical requirements going undetected due to confusions in functional responsibility.

23. The majority of ICT tasks have been formalised and updated, and roles have been assigned to ICT personnel, with their responsibilities clearly stated. However, there was understaffing and over-reliance on United Nations Volunteer (UNV) staff. With the current level of staffing shortage, the Mission may be unable to meet the demands placed upon it, should there be a major incident or escalation of security threats. The issue pertaining to over-reliance on UNV staff was particularly significant in the majority of the regional offices, where many asset managers were UNV staff. This condition could have a significant impact on service continuity at the end of each UNV cycle. In addition, there was no evidence of a succession planning process to mitigate the risks posed by such a situation.

24. OIOS found a documented procedure on 'checking in and out', which is the process for administering newcomers and departing staff. However, this document did not contain the requirement to ensure that important records/sensitive data are appropriately handed over on departure of personnel from the Mission. There is a risk that the location of important records/data are not known or not handed over and held securely. This could result in unauthorised access to privileged data when employment has ended or, the lack of smooth continuation of business-critical operations.

Recommendations 8 to 10

The MONUC Office of Mission Support should:

(8) Undertake a review of its staffing requirements to ensure that the ICT operational requirements of the Mission can be met.

(9) Develop a succession planning process so that there is early identification and solutions of staffing requirements that may impact the future operations of the Mission.

(10) Develop and implement procedures and guidelines to ensure that officers hand over all important/sensitive documentation upon their separation from the Mission.

25. *The MONUC Office of Mission Support accepted recommendation 8 and stated that Staffing requirements are regularly reviewed to meet operational requirements. Recommendation 8 remains open pending documented evidence of the recent review conducted for the determination of ICT staffing requirements.*

26. *The MONUC Office of Mission Support did not accept recommendation 9 and stated that the fluid situation in the mission makes it very difficult to project for long-term succession planning. UNVs rotate every 6 months and management only becomes aware of their decision within the last two months of their tenure. In the opinion of OIOS, MONUC needs to establish a succession planning process to ensure the least possible disruption to MONUC and therefore the Mission's effectiveness for redeployment of personnel. OIOS therefore*

reiterates recommendation 9, which remains open pending the development of a succession planning process.

27. *The MONUC Office of Mission Support accepted recommendation 10 and stated that the archiving procedures will be included in the induction program for newcomers and in the checkout process. The requirement for handover of documentation will be reinforced via Administrative Circular by management.* Recommendation 10 remains open pending OIOS receipt of documented evidence of handover requirements and procedures for the separation process.

Limited deployment of the automated service management system

28. MONUC has in place a defined and structured problem management and resolution process with escalation procedures and a service desk system in place. The process uses an automated service management system called HP Open View (HPOV). This system is used to report, record, analyse and resolve service requests. Incident reports for significant problems are generated and submitted to the appropriate level of management. However, OIOS noted that the use of this system is limited to Kinshasa, and is not available to other Mission offices. This could limit the effectiveness and timeliness of service provision to the whole Mission.

Recommendation 11

(11) The MONUC Office of Mission Support should deploy the automated service management system (HPOV) to the entire Mission, to enhance the effectiveness and efficiency of ICT service help-desk.

29. *The MONUC Office of Mission Support accepted recommendation 11 and stated that HPOV license expires in December 2008 and MONUC will use open source software "One or Zero".* Recommendation 11 remains open pending receipt of evidence documenting the deployment of the automated service management system to the entire mission.

Limited implementation of data classification

30. The Department of Peacekeeping Operations and the Department of Field Support have issued a policy directive entitled "Record Management". This policy directive was originally issued in January 2006 and updated in December 2007 to take into account the provisions established in ST/SGB/2007/6 (Information Sensitivity, Classification and Handling), and provides guidance on how to address the taxonomy for information classification. OIOS noted that an officer has been dedicated within the records management unit to ensure the implementation of the bulletin. However, OIOS was informed that the records management unit is still faced with lack of cooperation from some units within the Mission which do not provide access to records, so that a determination can be made of the type of data/information held within these units. There is a risk

that records would not be adequately classified, which could result in their inadequate protection, and breaches in security and loss of information.

Recommendation 12

(12) The MONUC Office of Mission Support should improve awareness of ST/SGB/2007/6 (Information Sensitivity, Classification and Handling) and ensure that it is fully implemented to ensure correct classification and protection of data and information.

31. *The MONUC Office of Mission Support accepted recommendation 12 and stated that management will further increase awareness of the relevant ST/SGB. Recommendation 12 remains open pending receipt of evidence documenting the implementation of the awareness program on information sensitivity, classification and handling.*

Adequate ICT inventory management

32. ICT inventory management within the Mission was well established and defined. Procedures were found to be in place and there was an inventory of ICT assets.

A. Strategic management

MONUC has not established an ICT committee nor formalised its ICT strategy

33. MONUC faces significant constraints, due to its geographical spread and operational complexity. The ICT management has put in place an adequate system to respond to the day to day ICT demands of the Mission. However, concerning the longer term perspective, there was a need to further structure the governance over ICT operations to achieve the potential for ICT to enable Mission goals. For example, MONUC has not established an ICT committee, to ensure that ICT goals and requirements were discussed and decided upon at the appropriate management level. In fact, the MONUC CITS was in control of both the ICT strategic and operational processes. There was limited stakeholder involvement in ICT decision making which created risks of misalignment between CITS's and Mission's goals. In turn, a misalignment could lead to conflicts regarding priorities for resources allocation. The establishment of an ICT committee, as recommended with Rec. 3, would aid the ICT governance process.

34. MONUC/CITS had documented an ICT strategy for the Mission but this document was still in draft and had not been finalized. Delays in formalising this document could prevent the Mission from defining ICT priorities, allocate adequate resources, and ultimately have a negative impact on Mission's operations.

Recommendation 13

(13) The MONUC Office of Mission Support should finalize the MONUC ICT strategy.

35. *The MONUC Office of Mission Support accepted recommendation 13 and stated that the draft DFS ICT Strategy is used as a reference to aid decision making and providing guidelines in the Mission. Recommendation 13 remains open pending formalization of the draft Mission ICT strategy.*

MONUC ICT work plan not aligned with UN wide initiatives/projects.

36. The ICT work plans for the years 2007-08 and 2008-09 were reviewed. In general, the ICT work planning process was adequately managed and ensured adequate monitoring and control of ICT operations. However, UN wide initiatives/projects that may have an impact on the Mission, such as the ERP, CRM and ECM initiatives, were not considered during the work planning process. This gap could result in duplication of efforts, waste of resources and implementation of projects that are not in compliance with UNHQ ICT strategic direction.

Recommendation 14

(14) The MONUC Office of Mission Support should establish a process for integrating UN wide initiatives that may affect the ICT operations of the Mission into the operational planning process.

37. *The MONUC Office of Mission Support accepted recommendation 14 and stated that MONUC complies with UN wide initiatives that affect ICT operations. Recommendation 14 remains open pending receipt of evidence documenting the ICT operational planning process, including requirements to ensure integration of Mission-specific projects with UN-wide initiatives.*

Lack of formally defined thresholds to measure ICT performance

38. OIOS identified some processes for ICT performance and capacity monitoring within the Mission. However, where performance and capacity monitoring was undertaken, there were no standard or benchmarks to monitor against.

39. There was a framework for developing an ICT performance and capacity plan. However, this framework had not been fully formalised into a process for developing, reviewing and adjusting performance and infrastructure capacity. The process was ad hoc and reactive to issues, rather than proactive in nature. For instance, in response to the limitations on bandwidth resources, CITS wrote a data quality of service (QoS) report titled "MONUC satellite WAN links- steps towards efficient utilisation of bandwidth resources". These types of reviews were not done systematically as part of a formalised process. The risks associated with not having a formal process could lead to unexpected incidents due to lack of capacity; unavailability of systems due to a lack of proactive resource capacity

and performance planning; and failure to meet business requirements due to outdated performance and capacity plans and inadequate capacity.

40. The Mission's critical network assets were mainly located in Kinshasa and are now being monitored for security events. However, monitoring out of Kinshasa was limited. The Mission had procured performance monitoring tools, several of which had only been deployed in Kinshasa thus leaving the rest of the Mission exposed to unexpected incidents due to lack of regular monitoring.

Recommendation 15

(15) MONUC/CITS should document policies and procedures for systematic performance and capacity monitoring of the entire MONUC network.

41. *The MONUC Office of Mission Support accepted recommendation 15 and provided documented evidence of the policies and procedures for the performance and monitoring of the entire MONUC network.* Based on the action taken by the MONUC Office/Mission Support, recommendation 15 has been closed.

C. ICT security

Network lacks adequate bandwidth capacity

42. OIOS reviewed the systems that supported satellite and network operations. The controls around these operations, its constituent parts, interrelationships and the level of integration between the parts were clearly defined. In addition, resilience had been built into the network systems. MONUC adopted a multi layered defense approach for its network, which comprises of firewalls, proxy servers, internet content filtering software and appropriate access control measures.

43. The network was measured for capacity planning and performance measurement. However, it was subject to near capacity bandwidth utilisation. Bandwidth resources were faced with challenging priorities of usage from email, data backup, applications and the Internet. The use of more web-based applications also placed additional pressures on available resources and if not addressed will affect the Mission's ability to use the new ERP, CRM and ECM systems. In addition, bandwidth limitation was having significant impact on service operations, especially between the sectors and the headquarters in Kinshasa. For instance, bandwidth limitation made it difficult to achieve the implementation of an automated backup process across the whole Mission and affected the Mission's ability to automate data transfer across the network. However, the Mission is beginning to address the key issue of how the network links will continue to support the increasing demand. Currently there is a project in progress, which is looking at ways of streamlining the use of bandwidth resources and the development of a systematic process for prioritisation of bandwidth allocation. The Mission has also implemented a process (QoS) which

monitors network traffic flows, patterns, and ensures the allocation of bandwidth where it is required the most.

Lack of systematic vulnerability assessment of the Mission's network

44. In general, network activity was monitored to ensure the security and performance of the network. However, there was no program in place for periodic and systematic vulnerability assessments of the Mission's network, thus leaving the network vulnerable to the risks of security breaches.

Recommendation 16

(16) The MONUC Office of Mission Support should define and document policies and procedures for regular vulnerability assessments, and for the systematic monitoring of network security and performance. In addition, monitoring and assessment should be performed across the whole MONUC network.

45. *The MONUC Office of Mission Support accepted recommendation 16 and provided documented evidence of actions taken after the audit, in direct implementation of the recommendations issued. These actions included the following tasks: Cisco Security Agent solution; Cisco Network Admission Control; and Cisco MARS (Monitoring, Analysis, and Response System). Based on the action taken by the MONUC Office/Mission Support, recommendation 16 has been closed.*

46. The Mission procured several network security/monitoring tools, such as the intrusion prevention and detection modules (CISCO) and patch monitoring servers (WSUS). However, these tools were only deployed within the Mission headquarters in Kinshasa, and had not been consistently deployed across the whole Mission. This condition exposed the rest of the Mission to undetected security breaches and intrusions.

47. CITS had undertaken a review of network security and identified potential weaknesses within the system. OIOS requested during the audit to repeat the vulnerability scanning to confirm the security posture of the Mission's network. Weaknesses were identified which were critical to the efficient performance of the network and to the integrity of network functionality. CITS has either implemented or was in the process of implementing mitigating controls.

Recommendation 17

(17) The MONUC Office of Mission Support should ensure that actions are taken to address in full the weaknesses identified by the network vulnerability assessment.

48. *The MONUC Office of Mission Support accepted recommendation 17 and provided evidence of the monitoring performed on system vulnerabilities.*

Based on the action taken by the MONUC Office/Mission Support, recommendation 17 has been closed.

49. CITS/MONUC has developed a telephone billing system to monitor and process telephone usage across the Mission. However, the system is a web-based application implemented over an insecure network protocol hyper-text-transfer-protocol (Http), instead of secure-hyper-text-transfer-protocol (Https). Hence, the confidentiality and integrity of the data transmitted over the network could be easily breached.

Recommendation 18

(18) The MONUC Office of Mission Support should implement a secure standard protocol (i.e. https) for the communication channels supporting the telephone billing system and all other Mission critical applications.

50. *The MONUC Office of Mission Support accepted recommendation 18 and stated that other critical applications are already in https, and that also the telephone billing system will be implemented with https. Recommendation 18 remains open pending implementation of a secure standard protocol (https) for the telephone billing system.*

Lack of a business impact review process

51. Disaster recovery best practice suggests that organisations should regularly undertake a business impact review. This review should include an impact analysis and risk assessment of all critical operations, applications and systems. However, MONUC has not undertaken a systematic comprehensive Mission wide assessment, but had only an ad-hoc reactive process. A comprehensive business impact assessment is vital to the identification of potential risks and their impact on business processes and ICT systems critical to the Mission. The lack of a formal business impact review could result in unavailability of critical ICT resources, increased costs for continuity management; and prioritisation of service recovery not based on business needs.

Recommendations 19 and 20

The MONUC Office of Mission Support should:

(19) Define the ICT assets, and how each asset and its criticality impact the effective and efficient continuity of the Mission.

(20) Develop a risk management framework to enable the identification and control of the risks associated with information and information processing facilities within the Mission.

52. *The MONUC Office of Mission Support accepted recommendation 19 and provided documented evidence of actions taken after the audit, such as the*

business impact analysis conducted. Based on the action taken by the MONUC Office/Mission Support, recommendation 19 has been closed.

53. *The MONUC Office of Mission Support accepted recommendation 20 and provided evidence of the business impact analysis conducted. This analysis documented the criticality of information processing and its facilities as a benchmark for improvements.* Based on the action taken by the MONUC Office/Mission Support, recommendation 20 has been closed.

54. An assessment of the impact of environmental and natural hazards faced by the Mission had not been undertaken to determine the types of controls that could be put in place to mitigate the risks. For instance, OIOS was informed that personal computers (PC) had been damaged during heavy rainfall that had accessed some of the buildings. However, OIOS did not find that any precautionary equipment was being used, such as PC covers to reduce these risks.

Lack of a Mission-wide disaster recovery and business continuity planning process

55. DFS/DPKO have issued standard operating procedures and administrative instructions on disaster recovery and business continuity (2006-UNHQ-068498-DPKO Global DRBC Initiative). In addition, CITS was in the process of developing a disaster recovery and business continuity plan for the recovery of network facilities and computing services. However, this plan was only designed to protect Mission critical ICT services and to restore ICT services as quickly as possible. This document did not serve as a Mission plan that integrated ICT continuity with service continuity for the Mission as a whole. This creates inadequate business continuity planning for MONUC, which could lead to shortcomings in recovery plans, inappropriate recovery steps and the failure to recover business-critical systems and services in a timely manner due to lack of coordination between the functional areas and CITS.

Recommendations 21 to 23

The MONUC Office of Mission Support should:

(21) Document a formal business continuity/disaster recovery plan for the whole Mission.

(22) Include in the disaster recovery plan the impact of interruptions caused by any security incident and the action plan to deal with such incidents

(23) Document the financial, organisational and environmental resources required to address the needs of the Mission's disaster recovery and business continuity issues.

56. *The MONUC Office of Mission Support accepted recommendation 21 and stated that the Mission's disaster recovery and business continuity plans for information and communication technology are under review. The plan provides*

senior management and staff the necessary information and guidance for disaster recovery and business continuity activity and the ICT services that will be available. Recommendation 21 remains open pending receipt of the formally approved business continuity/disaster recovery plan.

57. *The MONUC Office of Mission Support accepted recommendation 22 and stated that the disaster scenarios and the recovery action plans are included in the Mission's disaster recovery and business continuity plan for information and communication technology. Recommendation 22 remains open pending receipt of the formally approved business continuity/disaster recovery plan, including the definition of the incident response plans.*

58. *The MONUC Office of Mission Support accepted recommendation 23 and stated that the Mission's business continuity plan addresses environmental, organizational and financial requirements needed. Recommendation 23 remains open pending receipt of evidence documenting how the financial, organizational and environmental resources have been included in the Mission's business continuity plan.*

Inadequate backup arrangements

59. Backup procedures within each installation were defined within the document titled "*MONUC Data Back up SOP*". MONUC currently backs up all production data, to tape. Incremental/differential backup of data is also replicated to the United Nations Logistical Base (UNLB) in Brindisi every other day, with full backup tapes sent to Brindisi once every two months. Backup arrangements covered both data and voice communication. MONUC was currently restricted to using manual back up processes because of limited bandwidth resources, which was restricting the use of automated backup tools that could enable remote backup over the network in a timelier manner.

60. The current backup arrangements had not been tested and there were no timetabled plans in the event of a major system loss. This condition exposes the Mission to serious risks, since the adequacy of the full backup arrangement will only be confirmed in the event of a disaster. Shortcomings in recovery plans could result in inappropriate recovery steps and processes, and the failure to recover business-critical systems and services in a timely manner.

61. Back-up tapes need to be retained in a secure environment to ensure data recovery in case of need. Therefore, it is good practice to locate backup disks off site to prevent destruction or compromise in event of a disaster. The MONUC backup tapes were kept in a safe in the same building that hosted the data and communication servers. This approach places the backup media in a situation where it may be impacted by the same risks that threaten the original data.

Recommendation 24

(24) The MONUC Office of Mission Support should schedule regular testing of the back up arrangements, designed for the Mission.

Recommendation 25

(25) The MONUC Office of Mission Support should ensure that back up tapes are not maintained in the same location as the servers that hold the original data. It is best practice to maintain back up tapes off site.

62. *The MONUC Office of Mission Support accepted recommendation 24 and stated that in addition to email notification of successful backups and log files, random backup tapes are taken out of the rotation cycle and are tested on a monthly basis to verify the validity of the backup tape.* Recommendation 24 remains open pending receipt of evidence documenting the results of a recent testing exercise.

63. *The MONUC Office of Mission Support did not accept recommendation 25 and stated that the two months backup tape rotation is in a different location than the server room, and is stored in a fireproof safe in a climate controlled container. The tapes are required to be in close proximity to the evacuation assembly point which is the same compound as the server room.* In the opinion of OIOS, it is important not to keep backup tapes in the same location as the servers because, in case of disaster, the tapes would be affected by the same adverse impact as the servers, and hence, the risks of not being able to recover data exist. OIOS therefore reiterates recommendation 25, which remains open pending implementation of the audit recommendation to maintain back up tapes in a different site location from the original data.

Inadequate controls to mitigate environmental hazards

64. The physical design of the MONUC ICT environment was found to take into account the risks associated with the logistics of the Mission. Physical security and access control measures were found to be adequate and where appropriate the sites had a 24 hour security presence, by way of physical security and/or closed circuit television (CCTV).

65. OIOS undertook site visits to seven of the Mission's ICT locations and observed that responsibility for controlling the physical security of ICT equipment was in place. In general, equipment was found to be securely located and adequate precautions existed to protect the assets. Computer equipment was located in restricted access areas. Network equipment such as servers, routers, cables, and trunking equipment were also in locked areas. However, the following weaknesses were noted:

- a) Fire equipment, in particular extinguishers, were not always strategically located for ease of access. The extinguishers were sometimes located several feet away from the room they were intended for. In addition, some of the extinguishers were water (H₂O) based instead of carbon dioxide (CO₂) based extinguishers. Industry recommends CO₂ based extinguishers for computer equipment because it does not leave behind harmful residues. H₂O based fire

extinguishers are not advised because water can be a dangerous extinguishing medium for computer equipment because of the risk of electrical shock.

- b) There were no raised floors in some of the server rooms. A raised server room floor allows for effective housekeeping and provides for a cold air distribution system to prevent equipment over heating.

Recommendations 26 and 27

MONUC Office of Mission Support should:

(26) Ensure that the correct fire extinguisher is installed and located near the equipment it is intended to protect.

(27) Ensure that server rooms have raised floors. In addition, the server rooms should be kept tidy with leads, cables secured, and unused equipment returned to the asset management unit.

66. *The MONUC Office of Mission Support accepted recommendation 26 and stated that the MONUC Fire Unit has raised requisition for 400 carbon dioxide fire extinguishers to replace the existing water based fire extinguisher near the CITS server rooms. Recommendation 26 remains open pending replacement of the water based extinguishers with carbon dioxide extinguishers.*

67. *The MONUC Office of Mission Support accepted recommendation 27 and stated that the MONUC server rooms in all locations have raised floors, and arrangements will be made to ensure constant tidiness. Based on the action taken by the MONUC Office/Mission Support, recommendation 27 has been closed.*

V. ACKNOWLEDGEMENT

68. We wish to express our appreciation to the Management and staff of the MONUC Office/Mission Support 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	The MONUC Office of Mission Support should review and update the current library of ICT policies and procedures for adequacy and relevance, and proceed to document policies and procedures where gaps have been identified. In addition, a formal process should be put in place to ensure the continuous update of ICT policies and procedures.	Governance	Medium	O	Review and update the current library of ICT policies and procedures.	Not provided
2	The MONUC Office of Mission Support should document a detailed project management framework to include standards for end user development, management and appropriate development tools.	Governance	Medium	O	Document the project management framework, including standard for end user development, management and tools.	31 December 2008
3	The MONUC Office of Mission Support should establish a local ICT committee in line with ST/SGB/2003/17, to maintain and update information on departmental systems, resources and assets, and existing systems; to confirm the cost effectiveness of information systems; and ensure that standard methodologies are consistently used for information and communication technology projects.	Governance	Medium	O	Establish a local ICT Committee in line with ST/SGB/2003/17, and issue terms of reference for the review of departmental systems, projects, and their cost effectiveness.	31 December 2008

Recom. no.	Recommendation	Risk category	Risk rating	C/O	Actions needed to close recommendation	Implementation date?
4	The MONUC Office of Mission Support should undertake a review of all current in-house developed systems and determine whether they will integrate into the ERP, CRM and ECM initiatives, being undertaken at the Secretariat.	Operational	Medium	O	Assess all current in-house developed applications, to determine whether they will integrate into the ERP, CRM, and ECM initiatives.	Not provided
5	The MONUC Office of Mission Support should document a procedure to ensure that before any future development of a system application, an assessment should be undertaken to verify that the same functionality would not be provided by the ERP, CRM and ECM initiatives.	Governance	Medium	O	Document a procedure to ensure that before any new ICT development, an assessment is undertaken to verify that the same functionality would not be provided by the ERP, CRM, and ECM initiatives.	Not provided
6	The MONUC Office of Mission Support should establish a process whereby the ICT requirements of Mission sites can be met through integrated working practices or sharing of local developments between different Missions, to prevent duplication, waste and inefficiencies.	Governance	Medium	O	Document the E-portal procedure, requiring locally developed ICT projects to integrate and share working practices between Missions.	Not provided
7	The MONUC Office of Mission Support should ensure that ICT duties are adequately segregated.	Governance	Medium	O	Document how ICT duties have been segregated within the Mission.	Not provided
8	The MONUC Office of Mission Support should undertake a review of its staffing requirements to ensure that the operational requirements of the Mission can be met.	Human Resources	Medium	O	Document the review conducted to determine the ICT staffing requirements.	Not provided
9	The MONUC Office of Mission Support should develop a succession planning process so that there is early identification and solutions to gaps in staffing requirements that may impact the future operations of the Mission.	Human Resources	Medium	O	Develop and document a succession planning process.	Not provided

Recom. no.	Recommendation	Risk category	Risk rating	C/O	Actions needed to close recommendation	Implementation date ²
10	The MONUC Office of Mission Support should develop local checking out guidelines to strengthen checking out procedures and to ensure that officers hand over all important/sensitive documentation upon their separation from the Mission.	Operational	Medium	O	Document the handovers requirements defined for the separation process.	Not provided
11	The MONUC Office of Mission Support should deploy the use of the automated service management system (HPOV) to the entire Mission, to enhance the effectiveness and efficiency of ICT service help-desk.	Operational	Medium	O	Deploy and document the automated service management system to the entire mission.	31 January 2009
12	The MONUC Office of Mission Support should improve awareness of ST/SGB/2007/6 (Information Sensitivity, Classification and Handling) and ensure that it is fully implemented to ensure correct classification and protection of data and information.	Operational	Medium	O	Implement and document the awareness programme on information sensitivity, classification and handling.	Not provided
13	The MONUC Office of Mission Support should finalize the MONUC ICT strategy.	Strategy	Medium	O	Formalize the draft Mission ICT Strategy.	Not provided
14	The MONUC Office of Mission Support should establish a process for integrating UN wide initiatives that may affect the ICT operations of the Mission into the operational planning process.	Information Resources	Medium	O	Document the ICT operational planning process, including requirements to ensure integration of Mission-specific projects with UN-wide initiatives.	Not provided
15	The MONUC Office of Mission Support should document policies and procedures for the systematic performance and capacity monitoring of the entire MONUC network.	Information Resources	Medium	C	Action completed.	Implemented

Recom. no.	Recommendation	Risk category	Risk rating	C/O¹	Actions needed to close recommendation	Implementation date²
16	The MONUC Office of Mission Support should define and document policies and procedures for regular vulnerability assessments, and for the systematic monitoring of network security and performance. In addition, monitoring and assessments should be performed across the whole MONUC network.	Information Resources	Medium	C	Action completed.	Implemented
17	The MONUC Office of Mission Support should ensure that actions are taken to address in full the weaknesses identified by the network vulnerability assessment.	Information Resources	Medium	C	Action completed	Implemented
18	The MONUC Office of Mission Support should implement a secure standard protocol (i.e. https) for the communication channels supporting the telephone billing system, and all other Mission critical applications.	Information Resources	High	O	Implement the secure standard protocol for communication (HTTPS), for the telephone billing system.	31 December 2008
19	The MONUC Office of Mission Support should define the ICT assets, and how each asset and its criticality impact the effective and efficient continuity of the Mission.	Information Resources	Medium	C	Action completed	Implemented
20	The MONUC Office of Mission Support should develop a risk management framework to enable the identification and control of the risks associated with information and information processing facilities within the Mission.	Governance	Medium	C	Action completed	Implemented
21	The MONUC Office of Mission Support should document a formal business continuity and disaster recovery plan for the whole Mission.	Information Resources	High	O	Document and approve the business continuity and disaster recovery plan for the entire Mission.	31 December 2008

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
22	The MONUC Office of Mission Support should include within the disaster recovery plan the impact of interruptions caused by any security incident and the action plan to deal with such incidents.	Information Resources	Medium	O	Document and approve the business continuity and disaster recovery plan for the entire Mission, including the incident response plans.	Not provided
23	The MONUC Office of Mission Support should document the financial, organisational and environmental resources required necessary to address the needs of the Mission's disaster recovery and business continuity issues.	Information Resources	Medium	O	Document the financial, organizational and environmental resources within the Mission's business continuity plan.	Not provided
24	The MONUC Office of Mission Support should schedule regular testing of the backup arrangements, designed for the Mission.	Information Resources	Medium	O	Document the results of a recent testing exercise.	Not provided
25	The MONUC Office of Mission Support should ensure that back up tapes are not maintained in the same location as the servers that hold the original data. It is best practice to maintain backup tapes off site.	Information Resources	Medium	O	Establish a second location for the safe-keeping of back-up tapes.	Not provided
26	The MONUC Office of Mission Support should ensure that the correct fire extinguisher is installed and located near the equipment it is intended to protect.	Information Resources	Medium	O	Replace the H20 extinguishers with Co@ extinguishers.	Not provided.
27	The MONUC Office of Mission Support should ensure that server rooms have raised floors. In addition, the server rooms should be kept tidy with leads, cables secured, and unused equipment returned to the asset management unit.	Information Resources	Low	C	Action completed	Implemented.

1. C = closed, O = open

2. Date provided by MONUC in response to recommendations.