



INTERNAL AUDIT DIVISION

AUDIT REPORT/2013/019

Audit of the information and communications technology (ICT) infrastructure supporting the implementation of IPSAS and Umoja

Overall results relating to the adequacy and effectiveness of the planning, configuration and support of the ICT infrastructure for the implementation of IPSAS and Umoja were initially assessed as unsatisfactory. Implementation of ten important and three critical recommendations remain in progress

FINAL OVERALL RATING: UNSATISFACTORY

19 March 2013

Assignment No. AT2012/610/01

CONTENTS

	<i>Page</i>
I. BACKGROUND	1
II. OBJECTIVE AND SCOPE	2
III. AUDIT RESULTS	2
A. Information technology infrastructure supporting the business objectives of the Organization	3-12
IV. ACKNOWLEDGEMENT	12

ANNEX I Audit recommendations

AUDIT REPORT

Audit of the information and communications technology (ICT) infrastructure supporting the implementation of IPSAS and Umoja

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of the information and communications technology (ICT) infrastructure supporting the implementation of the International Public Sector Accounting Standards (IPSAS) and Umoja (the new enterprise resource planning system of the United Nations Secretariat). The readiness of ICT infrastructure hosting the applications that process and store data relating to IPSAS and Umoja is critical for the successful implementation of these enterprise-wide initiatives.
2. In accordance with its mandate, OIOS provides assurance and advice on the adequacy and effectiveness of the United Nations internal control system, the primary objectives of which are to ensure (a) efficient and effective operations; (b) accurate financial and operational reporting; (c) safeguarding of assets; and (d) compliance with mandates, regulations and rules.
3. Given the delay in the implementation of the Umoja project, the Organization had taken a transitional measure to calculate IPSAS opening balances using existing ICT systems (Galileo, Mercury, Sun Systems, Integrated Management Information System (IMIS) and other supporting applications).
4. The Department of Management (DM), in accordance with the Secretary-General's bulletin ST/SGB/2010/9, "formulates policies and procedures and provides strategic guidance, direction and support to all entities of the Secretariat in finance, budget, human resources, and physical resources (support operations and services)". The Under-Secretary-General of DM is the project owner of Umoja.
5. The Office of Information and Communications Technology (OICT) of DM provides support for the enterprise-wide systems and infrastructure. This includes planning and developing the overall infrastructure architecture, encompassing the communications networks and data centres of the Organization. OICT operates two data centres at United Nations Headquarters (UNHQ), providing infrastructure and services for some IPSAS-related applications. In addition, OICT designed two enterprise data centres for the support of enterprise applications in the main locations of the United Nations Global Service Centre (UNGSC), at the United Nations Logistics Base in Brindisi (UNLB), and at the United Nations Support Base in Valencia (UNSB-V). The Communications and Information Technology Sections (CITS) of UNLB and UNSB-V operate the enterprise and local data centres established in UNLB and UNSB-V and maintain communications with the field.
6. The Information and Communications Technology Division (ICTD) in the Department of Field Support (DFS) is responsible for supporting the work of OICT in: (i) establishing ICT architecture and standards; (ii) planning and implementing major infrastructure improvements for field operations; (iii) implementing and supporting Organization-wide applications and major shared field applications; (iv) providing centralized ICT project management support; (v) coordinating disaster recovery and business continuity planning for the field; and (vi) maintaining strategic oversight of the enterprise data centres and major communications facilities, including review and approval of strategic directions.
7. Comments provided by DM, UNLB, UNSB-V and the Umoja Office are incorporated in italics.

II. OBJECTIVE AND SCOPE

8. The audit was conducted to assess the adequacy and effectiveness of the governance, risk management and control processes established by the Secretariat in providing reasonable assurance regarding the **effective planning, configuration and support of the ICT infrastructure for the implementation of IPSAS and Umoja**.

9. This audit was included in the 2012 OIOS risk-based work plan because the readiness of ICT infrastructure is critical for the success of IPSAS and Umoja implementation.

10. The key control tested for this audit was the **ICT infrastructure supporting the business objectives of the Organization**. For the purpose of this audit, OIOS defined this as the control that provides reasonable assurance that the ICT infrastructure established is adequately supporting the implementation of IPSAS and Umoja.

11. The key control was assessed for the control objectives shown in Table 1.

12. OIOS conducted this audit from June to October 2012. The audit covered the period from March 2011 to October 2012.

13. OIOS conducted an activity-level risk assessment to identify and assess specific risk exposures, and to confirm the relevance of the selected key controls in mitigating associated risks. Through interviews, analytical reviews and tests of controls, OIOS assessed the existence and adequacy of internal controls and conducted necessary tests to determine their effectiveness.

III. AUDIT RESULTS

14. The governance, risk management and control processes examined in the Secretariat were assessed as **unsatisfactory** in providing reasonable assurance regarding the **effective planning, configuration and support of the ICT infrastructure for the implementation of IPSAS and Umoja**.

15. OIOS made thirteen recommendations to address issues identified in the audit. OICT and DFS established primary and secondary data centres at UNHQ and at UNGSC, which is composed of UNLB and UNSB-V, with adequate network and data storage infrastructure to support the existing applications. A limited scope ISO-27001 certification was in place, covering network operations. Annual vulnerability assessments for network equipment were performed; however, security vulnerabilities of application servers were not included in these assessments. Disaster recovery plans for IPSAS-related applications were not documented and tested (except the asset management system, Galileo). Infrastructure capacity planning was based on the requirements of existing applications and bandwidth, and storage planning did not include Umoja's needs.

16. The overall rating is based on the assessment of key controls presented in Table 1 below. The final overall rating is **unsatisfactory** as implementation of ten important and three critical recommendations remains in progress.

Table 1: Assessment of key controls

Business objective	Key controls	Control objectives			
		Efficient and effective operations	Accurate financial and operational reporting	Safeguarding of assets	Compliance with mandates, regulations and rules
Effective planning, configuration and support of the ICT infrastructure for the implementation of IPSAS and Umoja	Information technology infrastructure supporting the business objectives of the Organization	Unsatisfactory	Partially satisfactory	Unsatisfactory	Partially satisfactory
FINAL OVERALL RATING: UNSATISFACTORY					

A. Information technology infrastructure supporting the business objectives of the Organization

A.I. UNHQ ICT Infrastructure

17. OIOS conducted a series of tests on the UNHQ ICT infrastructure supporting the applications that process and store data relating to IPSAS and Umoja, including: IMIS; Budget Information System (BIS); Operations Processing Integrated Control System (OPICS); Procure Plus; Nucleus and Nova. The results of these tests highlighted areas of risks in the ICT infrastructure hosting the main applications of the Secretariat, as summarized below under each area.

Inadequate physical and environment controls

18. OICT operated the Primary Technical Centre (PTC), located in the North Lawn Building of the United Nations Secretariat in New York. PTC was designed and built as part of the Capital Master Plan and became operational in 2010. OICT established a Secondary Technology Centre (STC) in a shared data centre facility located in Piscataway, New Jersey. STC acted as the disaster recovery site of some of the applications hosted in PTC. The two data centres were operated by the Network Operations Centre (NOC) team of the United Nations International Computing Centre (UNICC).

19. Although the majority of the controls were in place, OIOS identified some issues, as follows:

- (i) Tests of the power system in the PTC had not been conducted since 2010; and
- (ii) Some boxes and unused material were kept inside the data centre which increased the risk of fire. OICT explained that although it had made repeated requests to obtain a storage space on the premises, this space was not yet available. Consequently, materials for immediate deployment were kept temporarily in the data centre.

<p>(1) OICT should, in coordination with the Facilities Management Service of DM: (i) plan a power test of the primary technology centre; and (ii) remove flammable materials kept in</p>
--

the data centres.

OICT accepted recommendation 1 and stated that a power test will be scheduled following issuance of the new disaster recovery plan, and that it will remove flammable materials following the provision of adequate storage by Facilities Management Service of DM, as the Capital Master Plan project progresses. Recommendation 1 remains open pending receipt of the results of the power test, and evidence of the controls put in place to prevent flammable materials from being kept in data centres.

IMIS servers not supported with a long term contract

20. The IMIS servers were maintained in accordance with a contract that expired in July 2012. For IMIS to function as expected, it requires specific hardware. This hardware and its associated operating system were no longer supported by the manufacturer, Hewlett-Packard, since 2009. OICT estimated that IMIS should be supported for at least 8 more years until the Umoja system is fully implemented across the Organization. OICT raised a requisition for establishing a long term systems contract to secure spare parts and services for the required IMIS hardware. This procurement exercise was still in progress. Longer delays in the procurement process and potential hardware failures of the IMIS servers across the Organization might have a negative impact during the implementation of IPSAS.

(2) OICT should develop a contingency plan to ensure the availability of spare parts and continuity of support for the obsolete IMIS servers pending the completion of the procurement process.

OICT accepted recommendation 2 and stated that current server maintenance agreement has been extended until 31 March 2013 and the establishment of long term agreement is in progress with the Procurement Division. Recommendation 2 remains open pending receipt of the documented inventory of the spare hardware stored by OICT for supporting IMIS and establishment of the long term contract.

Inadequate staffing in support of ICT infrastructure and lack of contingency planning

21. OICT performed an assessment of the staffing resources required for the support of IMIS infrastructure in the Offices Away from Headquarters (OAH), and reported the following results to the IPSAS Steering Committee:

- a. The United Nations Office at Vienna (UNOV) lost extra budgetary funding for the two IMIS infrastructure support staff (one P-3 and one GS-6);
- b. The Economic and Social Commission for Asia and the Pacific (ESCAP) had the smallest IMIS infrastructure support team with only one GS-6 who will retire in 2015; and
- c. The UNHQ infrastructure staff with IMIS knowledge moved to other projects.

22. In addition, OIOS identified inadequate staffing, lack of knowledge transfer and training in the following areas which might have a negative impact on the continuity of the support of ICT infrastructure:

- (i) In the OICT IMIS server management team, there were only two staff members trained for the support of IMIS servers (HP Unix systems). This staff was not fully dedicated to

this function and there was no contingency plan in place to facilitate knowledge transfer; and

- (ii) Until recently, several Nova applications were managed independently by the departments owning the applications. OICT initiated actions to consolidate the support for Nova applications and established service level agreements with some of the client departments. However, the transition was not complete and there was only one staff in OICT who had adequate knowledge of the system infrastructure.

(3) OICT should: (i) in coordination with the Offices Away from Headquarters, formalize the requirement for ensuring support of the IMIS infrastructure in the ICT budget proposals; and (ii) ensure continuity of infrastructure support by allocating adequate staffing, training the staff and facilitating knowledge transfer.

OICT accepted recommendation 3 and stated that service level agreements for Nova could be established provided that a contract to sustain maintenance of Nova is put in place. Recommendation 3 remains open pending receipt of the documented: (i) requirements for IMIS infrastructure included in the budget proposal; and (ii) training, knowledge transfer and staffing plans.

Lack of disaster recovery planning and testing

23. OICT used the STC for disaster recovery (DR) purposes. IMIS data stored in PTC was replicated to storage devices in STC. OICT run the applications on redundant servers with redundant disks, CPU, memory, power, and network cards. The network connectivity between PTC and STC was redundant and adequate for DR purposes. OICT allocated staff resources to automate the IMIS manual failover procedures and planned to test the new procedures as part of this initiative. However, there was no documented DR plan covering all applications hosted in the data centres and tests were not performed for DR purposes. Additionally, Nova applications did not have DR instances in STC.

(4) OICT, in coordination with the application owners (i.e IMIS, OPICS, Procure Plus, BIS, Swift, etc.) should: (i) document the ICT disaster recovery plans for each application; and (ii) test and revise them on an annual basis.

OICT accepted recommendation 4 and stated that it will coordinate efforts related to disaster recovery planning of the mentioned applications (IMIS, OPICS, Procure Plus, BIS, Swift, etc.). Recommendation 4 remains open pending receipt of the documented disaster recovery plans for the above-mentioned applications.

ICT security risks not mitigated

24. OICT maintained an information security management system and its network infrastructure has been certified against an international standard for security management (ISO-27001). However, the scope of the certification was limited to network assets and did not cover the application servers in the data centres. OICT performed an ICT security risk assessment for the network in May 2011 and documented high and medium security risks. The mitigation activities identified in the risk report had not yet been implemented.

25. As part of this audit, OIOS coordinated with OICT the conduct of vulnerability scans on the servers supporting IMIS, OPICS, BIS, Nova and Procure Plus. The results of these tests are shown in

Table 2. OICT provided the vulnerability report to each system owner, and actions were initiated for resolving the issues identified.

Table 2: Results of vulnerability tests conducted on the main application servers

	Number of high risk vulnerabilities identified	Number of medium risk vulnerabilities identified
IMIS	1	1
BIS	0	3
NOVA	3	13
OPICS	3	4
Procure Plus	Not assessed due to upgrade	Not assessed

(5) OICT should: (i) mitigate the vulnerabilities identified in the risk assessments of the network and application servers; and (ii) perform periodic vulnerability scans and risk assessments for IMIS, BIS, Procure Plus, and OPICS servers.

OICT accepted recommendation 5. Recommendation 5 remains open pending receipt of the results of the vulnerability tests performed and corresponding mitigation actions implemented.

Use of generic and shared accounts

26. Third party remote administration of servers or network equipment was adequate. Support for the equipment was performed on-site with the supervision of OICT system administrators. However, the results of the vulnerability test showed that default access credentials were used on some servers (i.e., servers supporting the network management), which increased the risk of disclosure of server configuration information. Additionally, IMIS database administrators used a shared account for database administration and activity logs of these powerful accounts were not monitored.

27. The check-out procedure established by OICT did not include a formal control to ensure the removal of access rights from staff members that were either leaving the Organization or moving to other assignments. This condition could cause unauthorized access to the systems.

(6) OICT should: (i) change the default credentials used on the servers; (ii) document its check-out procedure, including checks for removal of access rights from the systems; and (iii) establish procedures to prohibit the use of generic and shared accounts for system and database management.

OICT accepted recommendation 6 and stated that it will implement the recommendation by the end of 2013. Recommendation 6 remains open pending receipt of documentation showing the controls implemented for default passwords, check-out process, and use of generic/shared accounts.

Risk of unauthorized access, security vulnerabilities and lack of disaster recovery planning in Nova applications

28. The Nova platform supported more than 10 applications being used by DFS, OPPBA, the Umoja Office, OICT, the Capital Master Plan, the Department of Political Affairs (DPA) and other departments. There was no central coordination or contractual framework for the application support, infrastructure management, documentation, maintenance and enhancement efforts of Nova applications across the UN Secretariat. Each office had been hiring individual contractors to meet its needs. OIOS identified several weaknesses due to this approach such as: (i) security vulnerabilities; (ii) lack of disaster recovery instance

in STC; (iii) lack of disaster recovery plans; and (iv) lack of adequate documentation or knowledge transfer to the OICT staff managing the infrastructure components (hosting the servers). In order to mitigate these risks, OICT developed a Statement of Work (SOW) to establish a contractual framework for the support of Nova applications and was working with the Procurement Division for completion of the procurement exercise.

29. OIOS reviewed the SOW prepared by OICT and noted that “security enhancements” were not included in the requirements for Nova support. The vulnerability scans run on Nova servers indicated high and medium risk vulnerabilities. Additionally, access credentials for the shared database were assigned to multiple administrators in OICT, DFS and OPPBA, without clear roles and responsibilities between them. Database administrators used a single shared account having access to all the tables, including those containing other departments’ data. This condition increased the risk of unauthorized access to sensitive information. In addition, certain database components were unnecessarily installed on the Nova application servers creating complexity to the infrastructure and introducing security vulnerabilities associated with the unused components. These vulnerabilities need to be mitigated by implementing security controls in the Nova system.

30. Additionally, the ICT infrastructure supporting the Nova application servers was not uniform (i.e., different versions of system software “ColdFusion” installed in OPPBA application servers), creating a complex and difficult ICT environment to manage.

(7) OICT should, in coordination with DFS and OPPBA: (i) define the minimum database access requirements of each department to manage system components of Nova and restrict the access rights of departmental database administrators; (ii) establish monitoring and change management controls for the shared components of Nova based applications; (iii) remove unused local databases from the application servers; and (iv) upgrade the system software of Nova based applications to ensure that a standard configuration is in place; and (v) ensure that security vulnerabilities are mitigated and disaster recovery plans of Nova applications are completed and tested.

OICT accepted recommendation 7 stating that until a proper contractual vehicle is in place for the maintenance and support of the Nova based applications, the actions recommended cannot be implemented. OICT further indicated that it has been working in coordination with the Procurement Division on a request for proposal (RFP) for Nova maintenance and support. The work plan of the original RFP was intended to be completed by January 2013, but it is still in progress. Until this process is completed, OICT does not have the capacity to initiate proper support and governance regarding Nova applications. Recommendation 7 remains open pending the completion of the procurement process currently in progress and the implementation of the actions recommended.

Lack of a configuration management database

31. The change management process implemented by OICT for ICT infrastructure was manual. Procedures were documented and change management logs existed. However, OICT did not utilize a configuration management database (CMDB) tool for monitoring the various components supporting applications and services in the ICT infrastructure. For example, due to the absence of a fully functional CMDB, OICT could not provide the list of equipment failures of the server model used for IMIS. Similarly, IPSAS related applications were not defined as configuration items. Therefore, it was not possible to generate a report with the list of servers supporting the IPSAS related applications and their configuration information. The absence of a fully functional CMDB prevented OICT from adequately

assessing, monitoring and reporting on the risks associated with vulnerabilities, incidents, problems, maintenance activities, changes, and dependencies of the ICT infrastructure supporting IMIS.

(8) OICT should implement a configuration management database for monitoring and reporting on the potential risks associated with the complex ICT environment.

OICT accepted recommendation 8 and stated that it is exploring alternative systems that will allow management of a configuration management database and expressed its concerns about the full implementation due to lack of resources. Recommendation 8 remains open pending receipt of evidence documenting implementation of the configuration management database (or equivalent) that links incidents, problems and risks to the ICT assets.

Potential performance issues of IMIS

32. Capacity and performance of ICT infrastructure were adequately monitored by OICT. In addition, feedback obtained from application owners confirmed the adequacy of infrastructure performance.

33. Concerns existed on the future performance of IMIS because of the increasing size of its database and the limitations in the availability of hardware and upgrades. The IMIS database has grown over the years, and its current size is 90 GB. Based on past trends, OICT estimated that the size of the database will double in two years, reaching 180 GB. The performance issues due to the growing size of the IMIS database were resolved by upgrading to more powerful hardware in the past. However, source code continued to be dependent on the operating system and new servers in the market did not support this old operating system. As a result of this limitation, OICT expected that in the near future the application would become slower and overnight programs would not have enough time to complete their processing. OPPBA stated that it had analyzed these and long running batches pertain to human resources data (time and attendance) not finance. OICT stated that funding is not available to enhance IMIS performance and it is not in a position to re-engineer the long running batches or archiving the data. OIOS does not make a recommendation at this point, since the involved parties are monitoring the risks associated with IMIS performance.

A.II. United Nations logistics support bases

Procedures were in draft and not reviewed as required

34. UNLB and UNSV-B had documented policies, standard operating procedures (SOP) and operational level agreements (OLA) for managing ICT infrastructure. However, some of the SOPs and OLAs were in draft form, not dated/signed, or not reviewed as required. Shared sites contained inconsistent copies of these files. UNLB and UNSB-V stated that a process had been implemented to harmonize the establishment of standard operating procedures across ICT at the UN logistics bases. Therefore, given that UNLB and UNSB-V have started the implementation of the required actions, OIOS is not making any additional recommendations at this stage.

Power interruption risk at the UNLB enterprise data centre

35. UNLB provided hosting, maintenance and support for the IPSAS-related applications Galileo, Mercury, Field Support Suite (FSS), and Business Objects, as well as storage for the data replications of the SUN systems and Lotus Notes databases installed in the missions. Additionally, some enterprise applications provided by OICT were hosted in UNLB. The Data Centre Support Section of UNLB managed and supported the servers, storage, network and systems software with documented procedures. Tier-1 support was provided by the Network Control Centre (NCC) team of UNICC. The data centre

infrastructure and support services were certified with the international standard for security management ISO-27001.

36. UNLB hub consisted of two data centres, for DFS applications and enterprise applications respectively. In addition, a new data centre has being built.

37. Power and cooling systems were redundant, except for one of the rows in the data centre hosting enterprise applications, which was supported by only one uninterruptible power source (UPS). The doors of some of the racks in this data centre were not locked and one of the data centre's walls was glass, which might have a negative impact on security and cooling. UNLB explained that these risks will be mitigated with the migration to the new data centre currently under construction. Given the imminent relocation to the new data centre, OIOS is not making any recommendation on this matter.

Lack of unified configuration management database

38. Changes to the ICT infrastructure installed in the UN logistics bases were adequately managed using a change management tool implemented in Lotus Notes. However, UNLB and UNSV-B used different applications for recording the information pertaining to their ICT assets (configuration items). The system used in UNLB provided flexible reporting by grouping the configuration items by application name, location, model, technical manufacturer, operating system and network address. While UNLB and UNSB-V constituted two components of a unified global entity (the United Nations Global Support Centre, UNGSC), the use of two distinct applications for recording data related to ICT assets lead to fragmented data sources and difficulties for monitoring and reporting. UNLB and UNSB-V stated that UNGSC had started a project for the implementation of a centralized configuration management system.

Lack of security assessments of application servers and security event management

39. UNLB established an information security management system certified with the international standard for security management ISO-27001, adopted by the United Nations Secretariat. However, the applications were not covered in the scope of the certification. UNSB-V did not have its own information security management system and its ICT infrastructure had not been certified, although it was part of the UNGSC hub hosting the enterprise applications.

40. While a security assessment had been conducted on the production environment of the FSS, other IPSAS-related applications had not yet been subject to such assessments.

(9) UNLB and UNSB-V should: (i) extend the scope of the information security management system to include the ICT infrastructure of UNSB-V; and (ii) complete the security assessments of IPSAS related applications and mitigate any identified vulnerability.

UNLB and UNSB-V accepted recommendation 9 and stated that the process to extend the scope of information security management will be completed by the end of 2013. Recommendation 9 remains open pending receipt of the ISO certification covering UNSB-V and the results of the vulnerability tests and mitigation actions taken for IPSAS-related applications.

Incidents regarding the Umoja system were not adequately managed

41. UNLB and UNSB-V utilized a tool (iNeed) for incident management, and its service desk implemented and documented incident management procedures. However, these procedures did not cover the Umoja infrastructure, and there was no staff with adequate knowledge of it in UNSB-V. In November 2012, the Umoja Office established a contract with an external company for hosting and managed

services. The *Umoja Office* stated that incident management requirements were addressed with this contract and that the external company determined that it will be able to meet the contractual obligations without a team on premises in Valencia. Rather, primary support will be provided from New York and other remote locations. The preparation of the documentation related to monitoring and support procedures has been started. Based on the information provided, OIOS is not making any additional recommendations on this matter.

Incomplete disaster recovery planning and testing

42. The disaster recovery plan for UNLB and UNSB-V was not complete. The plan covered satellite systems, data centre and Galileo. A validation exercise was conducted to evaluate the DR readiness of both UNSB-V and UNLB. This exercise simulated the full interruption of Galileo services to the United Nations Interim Force in Lebanon (UNIFIL). The United Nations Secretariat decided to use FSS, Mercury and Galileo for supporting the implementation of IPSAS and Umoja. However, a disaster recovery plan for Mercury, FSS, Business Objects (reporting tool of Mercury and Galileo), and Sun systems was not documented and tested.

(10) UNLB and UNSB-V should complete and test disaster recovery plans, including for Mercury, Field Support Suite, Business Objects, Sun and the other applications supporting the implementation of IPSAS.

UNLB and UNSB-V accepted recommendation 10 and stated that tests of the disaster recovery plans are expected to be conducted and completed by 31 March 2013. Recommendation 10 remains open pending receipt of the disaster recovery plans and test results.

Umoja network infrastructure and undefined management structure of the network

43. In accordance with the Secretary-General's report A/66/381, Umoja will be hosted at the enterprise data centres in UNLB and UNSB-V. The contract for hosting and system administration services of Umoja was awarded to an outside company (HCL Technologies). This company will be responsible for supplying and installing all components of the physical infrastructure in support of the entire Umoja system architecture and SAP operations at the operating system, database, and basis levels.

44. As of October 2012, OICT had completed the installation of the required security zoning infrastructure in both Valencia and Brindisi enterprise data centres, and the application acceleration/front-end environment. However, the Umoja production infrastructure was not yet fully implemented. In addition, a management structure was still being established for the execution of this process and the support of enterprise resource planning development and production environments, with the corresponding definition of roles and responsibilities.

45. As reported in the minutes of the Umoja Steering Committee of August 2012, OICT and ICTD/DFS had different opinions on the design of the network architecture in the infrastructure hosting environment. Should a consensus not be reached in a short period of time, the ASG/Umoja requested to be empowered to arbitrate and decide on the matter. OIOS noted that the presentation of this issue was not supported by adequate documentation describing the pros and cons of the two solutions being proposed by OICT and DFS. In OIOS' opinion, any decision made in the absence of a comparative analysis of the pros and cons associated with each solution may expose Umoja to undefined risks that could have a negative impact on the functioning of the system.

(11) OICT should, in coordination with DFS and the Umoja Office, ensure that a timely decision is made on the design of the network architecture for the infrastructure hosting environment of Umoja, by documenting: (i) the potential risks and impact of the network infrastructure options; and (ii) the roles and responsibilities for managing the infrastructure and hosting services.

OICT, DFS and the Umoja Office accepted recommendation 11 and stated that an agreement has been reached on this issue. However, the agreed approach is not yet documented. Recommendation 11 remains open pending receipt of the proposed solutions, roles and responsibilities for managing the infrastructure and hosting services.

Inadequate capacity planning for Umoja infrastructure

46. The storage, network bandwidth and disaster recovery requirements of Umoja production environment had not been communicated to UNGSC for advance capacity planning and implementation of required infrastructure changes in the UNGSC hub.

47. The Satellite Engineering Support Group in UNLB conducted a preliminary study for identifying the list of key requirements and changes needed for configuring the ICT infrastructure. The risks of not receiving the requirements and corresponding actions had been documented.

48. Best practices for the implementation of enterprise-wide systems such as enterprise resource planning systems require the identification of several details, including:

- (i) All the sites where the system will be deployed;
- (ii) Estimation of user concurrency for each site;
- (iii) Per user bandwidth requirements;
- (iv) Client access methods that might require additional virtual private network and licenses for secure communication;
- (v) Data volume to be replicated to disaster recovery site; and
- (vi) Storage requirements.

49. The Umoja team prepared a hardware sizing document which covered some of the elements listed above. However, in this document, missions were considered as single sites without differentiating the main offices of the missions, field sectors and team sites. Field sectors and team sites were usually not directly connected to the UNGSC (two hops satellite connections) and current network infrastructure of these mission offices might not be adequate to support Umoja. Additionally, the Umoja Office had not defined the client access methods, which will influence the bandwidth requirements and the number of virtual private network and secure communication licenses (Citrix). Bandwidth requirements to run the e-learning training for Umoja and the bandwidths required for data replication between primary and disaster recovery site were not assessed either. Storage requirements were not documented in the sizing document.

(12) The Umoja Office should, in coordination with DFS and OICT, define the details related to: (i) the sites (i.e., field sectors, team sites) where Umoja will be deployed with an estimation of user concurrency for each site; (ii) per user bandwidth requirements; (iii) SAP interfaces to be deployed; (iv) storage requirements; (v) data volume to be replicated to the disaster recovery site; and (vi) the number of Citrix licenses that will be needed to access SAP from some field offices.

OICT and the Umoja Office accepted recommendation 12. The Umoja Office stated that the ongoing decision process surrounding the choice of client access methods will help define the final bandwidth requirements, and number and nature of licenses. Umoja's anticipated storage requirements are documented in the materials supporting the hardware sizing exercise. Recommendation 12 remains open pending receipt of the documented requirements for bandwidth (including field sector; e-learning; and data replication requirements), storage, and license requirements.

50. The Umoja help desk and incident management strategy took into consideration the alignment with the global support strategy. However, the help desk staffing requirements, training of the Umoja help desk staff and escalation procedures had not been planned or documented.

(13) The Umoja Office should document the help desk staffing requirements for Umoja production along with escalation procedures.

The Umoja Office accepted recommendation 13 and stated that notification and escalation procedures are being documented by the Umoja technical team and the external company. Recommendation 13 remains open pending receipt of the documentation of help desk requirements and escalation procedures.

IV. ACKNOWLEDGEMENT

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



Mr. David Kanja, Assistant Secretary-General
Office of Internal Oversight Services

STATUS OF AUDIT RECOMMENDATIONS

Assignment noAT2012/610/01 – Audit of the information and communications technology (ICT) infrastructure supporting the implementation of IPSAS and Umoja

Recom. no.	Recommendation	Critical/ ¹ / important ²	C/ O ³	Actions needed to close recommendation	Implementation date ⁴
1	OICT should, in coordination with the Facilities Management Service of DM: (i) plan a power test of the primary technology centre; and (ii) remove flammable materials kept in the data centres.	Important	O	Recommendation 1 remains open pending receipt of the results of the power test, evidence of the controls put in place to prevent flammable materials from being kept in data centres.	31 December 2013
2	OICT should develop a contingency plan to ensure the availability of spare parts and continuity of support for the obsolete IMIS servers pending the completion of the procurement process.	Important	O	Recommendation 2 remains open pending receipt of the documented inventory of the spare hardware stored by OICT for supporting IMIS and extended contract.	30 June 2013
3	OICT should: (i) in coordination with the Offices Away from Headquarters, formalize the requirement for ensuring support of the IMIS infrastructure in the ICT budget proposals; and (ii) ensure continuity of infrastructure support by allocating adequate staffing, training the staff and facilitating knowledge transfer.	Important	O	Recommendation 3 remains open pending receipt of documented evidence of the: (i) requirements for IMIS infrastructure included in the budget proposal; and (ii) training, knowledge transfer and staff redundancy plans.	31 December 2014
4	OICT, in coordination with the application owners (i.e IMIS, OPICS, Procure Plus,	Critical	O	Recommendation 4 remains open pending receipt of the documented disaster recovery	31 December 2013

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

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

3 C = closed, O = open

4 Date provided by the clients in response to recommendations.

Recom. no.	Recommendation	Critical/ important ²	C/ O ³	Actions needed to close recommendation	Implementation date ⁴
5	<p>BIS, Swift, etc.) should: (i) document the ICT disaster recovery plans for each application; and (ii) test and revise them on an annual basis.</p> <p>OICT should: (i) mitigate the vulnerabilities identified in the risk assessments of the network and application servers; and (ii) perform periodic vulnerability scans and risk assessments for IMIS, BIS, Procure Plus, and OPICS servers.</p>	Important	O	<p>plans for the mentioned applications.</p> <p>Recommendation 5 remains open pending receipt of the results of the vulnerability tests performed and corresponding mitigation actions implemented.</p>	30 June 2014
6	<p>OICT should: (i) change the default credentials used on the servers; (ii) document its check-out procedure, including checks for removal of access rights from the systems; and (iii) establish procedures to prohibit the use of generic and shared accounts for system and database management.</p>	Important	O	<p>Recommendation 6 remains open pending receipt of documentation showing the controls implemented for default passwords, check-out process, and use of generic/shared accounts.</p>	31 December 2013
7	<p>OICT should, in coordination with DFS and OPPBA: (i) define the minimum database access requirements of each department to manage system components of Nova and restrict the access rights of departmental database administrators; (ii) establish monitoring and change management controls for the shared components of Nova based applications; (iii) remove unused local databases from the application servers; and (iv) upgrade the system software of Nova based applications to ensure that a standard configuration is in place. (v) ensure that security vulnerabilities are mitigated and disaster recovery plans of Nova</p>	Important	O	<p>Recommendation 7 remains open pending the completion of the procurement process currently in progress and the implementation of the actions recommended.</p>	31 December 2013

Recom. no.	Recommendation	Critical/ ¹ / important ²	C/ O ³	Actions needed to close recommendation	Implementation date ⁴
8	applications are completed and tested. OICT should implement a configuration management database for monitoring and reporting on the potential risks associated with the complex ICT environment.	Important	O	Recommendation 8 remains open pending receipt of evidence documenting the implementation of configuration management database (or equivalent) that links incidents, problems and risks to the ICT assets.	31 December 2014
9	UNLB and UNSB-V should: (i) extend the scope of the information security management system to include the ICT infrastructure of UNSB-V; and (ii) complete the security assessments of IPSAS related applications and mitigate any identified vulnerability	Important	O	Recommendation 9 remains open pending receipt of the ISO certification covering UNSB-V and the results of the vulnerability tests and mitigation actions taken for Galileo, Mercury, Business Objects, and Sun Systems.	31 December 2013
10	UNLB and UNSB-V should complete and test disaster recovery plans, including Mercury, Field Support Suite, Business Objects, Sun and the other applications supporting the implementation of IPSAS.	Critical	O	Recommendation 10 remains open pending receipt of the disaster recovery plans.	30 June 2013
11	OICT should, in coordination with DFS and the Umoja Office, ensure that a timely decision is made on the design of the network architecture for the infrastructure hosting environment of Umoja, by documenting: (i) the potential risks and impact of the network infrastructure options; and (ii) the roles and responsibilities for managing the infrastructure and hosting services.	Critical	O	Recommendation 11 remains open pending receipt of evidence documenting the evaluation of proposed solutions, roles and responsibilities.	30 June 2013
12	The Umoja Office should, in coordination with DFS and OICT, define the details related to: (i) the sites (i.e., field sectors, team sites) where Umoja will be deployed with an estimation of user concurrency for	Important	O	Recommendation 12 remains open pending receipt of the documented requirements for bandwidth (including field sectors; e-learning; and data replication requirements), storage, and license	30 June 2013

Recom. no.	Recommendation	Critical/ ¹ / important ²	C/ O ³	Actions needed to close recommendation	Implementation date ⁴
	each site; (ii) per user bandwidth requirements; (iii) SAP interfaces to be deployed; (iv) storage requirements; (v) data volume to be replicated to the disaster recovery site; and (vi) number of Citrix licenses that will be needed to access SAP from some field offices.			requirements.	
13	The Umoja Office should document the help desk staffing requirements for Umoja production along with escalation procedures	Important	O	Recommendation 13 remains open pending receipt of the documentation of help desk requirements and escalation procedures.	30 April 2013