



CONFIDENTIAL

Routine

TO: Mr. Gurpur Kumar, Deputy Director
A: Internal Audit Division, OIOS

DATE: 11 February 2013

REFERENCE: 2013-UNHQ-002574.01

THROUGH:
S/C DE:

FROM: Anthony Banbury, Assistant Secretary-General
DE: Department of Field Support

A handwritten signature in blue ink, appearing to be 'Anthony Banbury', written over the 'DE:' field of the 'FROM:' line.

SUBJECT: **AT2012/615/01 - Audit of the ICT infrastructure supporting the
OBJET: implementing IPSAS and Umoja**

I refer to your memorandum dated 25 January 2013, regarding the above-mentioned audit. We note that OIOS has substantially taken into account DFS' comments provided on 5 December 2012. The Department is providing additional comments on the recommendations that fall under the responsibility of the Under-Secretary-General for Field Support in the attached matrix. In formulating our response, we have conferred with the respective officials in DFS and their comments, where appropriate, have been incorporated in this reply.

cc: Yukio Takasu
Kiplin Perkins
Zachary Ikiara
Anna Halasan

AUDIT RECOMMENDATIONS

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

Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	OICT should, in coordination with the Facilities Management Service of DM: (i) plan a power test of the primary technology centre; (ii) remove flammable materials kept in the data centres; and (iii) activate biometric access controls in the Primary Technology Centre.	Important	N/A	N/A	N/A	We trust that OICT will provide its comments on this recommendation.
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	N/A	N/A	N/A	We trust that OICT will provide its comments on this recommendation.
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; (ii) ensure continuity of infrastructure support by allocating adequate support staff, training the staff and facilitating knowledge transfer; and (iii) establish service level agreements with those departments that manage the infrastructure components	Important	N/A	N/A	N/A	We trust that OICT will provide its comments on this recommendation.

¹ Critical recommendations address significant and/or pervasive deficiencies or weaknesses 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.

Rec. no.	Recommendation	Critical/ ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	(system software) of the Nova based applications.					
4	OICT, in coordination with the application owners of IMIS, BIS, OPICS, Nova Applications, Procure Plus, should: (i) document the ICT disaster recovery plans for each application; and (ii) test and revise them on an annual basis.	Critical	N/A	N/A	N/A	We trust that OICT will provide its comments on this recommendation.
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, Nova, Procure Plus, and OPICS servers.	Important	N/A	N/A	N/A	We trust that OICT will provide its comments on this recommendation.
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.	Important	N/A	N/A	N/A	We trust that OICT will provide its comments on this recommendation.
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	Important	N/A	N/A	N/A	DFS will provide any support that OICT requires to implement the recommendation.

Rec. no.	Recommendation	Critical/ Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
8	applications to ensure that a standard configuration is in place. OICT should implement a configuration management database for monitoring and reporting on the potential risks associated with the complex ICT environment.	Important	N/A	N/A	N/A	We trust that OICT will provide its comments on this recommendation.
9	OICT should allocate sufficient resources to enhance IMIS performance by re-engineering interactive codes and long running overnight programs and decrease the size of the database by archiving financial data.	Important	N/A	N/A	N/A	We trust that OICT will provide its comments on this recommendation.
10	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	Yes	Director, UNGSC	Fourth quarter of 2013	The United Nations Global Service Centre (UNGSC) has begun the process of extending the scope of its ISO 27000 certification to include the ICT infrastructure of the United Nations Support Base in Valencia. It is expected that the certification will be achieved by the fourth quarter of 2013. In addition, the ISO 27001 security awareness programme is ongoing in Valencia. UNGSC has also completed the statement of works for gap analysis and consultancy services for extended scope that will include the Valencia site in the certification.
11	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	Yes	Director, UNGSC	Second quarter of 2013	DFS comments are reflected in the draft report. The Department does not have any further comments.

Rec. no.	Recommendation	Critical/ Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
12	OICT should, in coordination with DFS and 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	N/A	N/A	N/A	DFS will provide any support that OICT requires to implement the recommendation.
13	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) number of Citrix licences that will be needed to access SAP from some field offices	Important	N/A	N/A	N/A	DFS will provide any support that Umoja Office requires to implement the recommendation.
14	The Umoja Office should document the help desk staffing requirements for Umoja production along with escalation procedures	Important	N/A	N/A	N/A	We trust that Umoja Office will provide its comments on this recommendation.

AUDIT RECOMMENDATIONS

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

Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	OICT should, in coordination with the Facilities Management Service of DM: (i) plan a power test of the primary technology centre; (ii) remove flammable materials kept in the data centres; and (iii) activate biometric access controls in the Primary Technology Centre.	Important	Yes	Chief, OICT/IMS	31 December 2013	The power test of the PTC will take place following issuance of the new disaster recovery plan. Regarding item (ii), OICT will remove all flammable material following provision of adequate storage by DM/OCSS/FMS as the CMP project progresses. Regarding item (iii), OICT uses card access control to the Primary Technology Centre. At present there is no established policy requiring OICT to deploy biometric access controls.
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	Yes	Chief, OICT/IMS	30 June 2013	The current server maintenance agreement has been extended until 31 March 2013. The establishment of the long term agreement for all duty stations' IMIS infrastructure is currently in progress with the Procurement Division.

¹ Critical recommendations address significant and/or pervasive deficiencies or weaknesses 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.

Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
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; (ii) ensure continuity of infrastructure support by allocating adequate support staff, training the staff and facilitating knowledge transfer; and (iii) establish service level agreements with those departments that manage the infrastructure components (system software) of the Nova based applications.	Important	Yes	Chief, OICT/IMS	31 December 2014	<p>OICT accepts items (i) and (ii) of the recommendation and has been in close contact with the Chiefs of ICT Services in the different Offices Away from Headquarters to ensure that adequate resource requests are included in their budget submission.</p> <p>OICT conditionally accepts item (iii) provided the Department is able to establish a contractual vehicle to sustain a maintenance and support contract for NOVA.</p> <p>OICT is currently working with the Procurement Division on a request for proposal for NOVA maintenance and support. The original RFP work plan was intended to be completed by mid-January 2013, but is still in progress. Completion of this procurement activity will provide the capacity to initiate proper support and governance regarding NOVA.</p>
4	OICT, in coordination with the application owners of IMIS, BIS, OPICS, Nova Applications, Procure Plus, should: (i) document the ICT disaster recovery plans for each application; and (ii) test and revise them on an annual basis.	Critical	Yes	Chief, OICT/IMS	31 December 2013	<p>OICT accepts the recommendation and will coordinate efforts related to IMIS, BIS, OPICS and Procure Plus.</p> <p>Insofar as NOVA is concerned, a proper contractual vehicle should be established as described in our response to recommendation 3 above. This will enable OICT coordination of maintenance and support for the NOVA-based applications.</p>

Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
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, Nova, Procure Plus, and OPICS servers.	Important	Yes	Chief, OICT/IMS	30 June 2014	OICT accepts this recommendation, except as it relates to NOVA. Insofar as NOVA is concerned, a proper contractual vehicle should be established for the maintenance and support of the NOVA-based applications as described in our response to recommendation 3 above.
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.	Important	Yes	Chief, OICT/IMS	31 December 2013	At the end of the fourth quarter of 2013, OICT will provide a list of actions taken in this regard.
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.	Important	Yes	Chief, OICT/IMS	31 December 2014	OICT conditionally accepts this recommendation provided a proper contractual vehicle is in place for the maintenance and support of the NOVA-based applications.
8	OICT should implement a configuration management database for monitoring and reporting on the potential risks associated with the complex ICT environment.	Important	Yes	Chief, OICT/IMS	31 December 2014	OICT is exploring alternative systems that will allow for the management of a configuration management database. However, implementation may be very limited given the lack of resources.

Rec. no.	Recommendation	Critical¹/ Important²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
9	OICT should allocate sufficient resources to enhance IMIS performance by re-engineering interactive codes and long running overnight programs and decrease the size of the database by archiving financial data.	Important	No	Not applicable	Not applicable	OICT does not accept this recommendation, as adequate funding for such work has not been identified. Additionally, OPPBA has analyzed the current performance of IMIS with regards to financial data and has indicated that re-engineering will provide no additional added benefit.
10	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				
11	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				
12	OICT should, in coordination with DFS and 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	Yes	Director, OICT	30 June 2013	An agreement has been reached regarding the design of the network infrastructure and hosting environment for Umoja. Documentation regarding the agreed solution will be provided.
13	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	Important	Yes	Team Leader, Technology Solutions	30 June 2013	OICT will provide any support that the Umoja Office requires to implement the recommendation.

Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	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) number of Citrix licenses that will be needed to access SAP from some field offices					<p>Umoja has worked closely with business and technical stakeholders to arrive at detailed estimates and analysis of expected user volumes. These estimates formed the basis of several sizing exercises aimed at determining the initial hardware sizing and network requirements for the Umoja infrastructure in Valencia and Brindisi, and have also been a factor in the ongoing decision process surrounding the choice of client access methods.</p> <ul style="list-style-type: none"> i. Detailed estimates of user counts and locations can be found in the documentation supporting the system sizing exercise, in material related to user and role definition (derived from user counts from legacy systems and analysis of where current processes are executed). ii. Bandwidth requirements for system usage are known, and are documented in material dating back to technical suitability exercises supporting the original software selection process for Umoja. It should be noted that actual bandwidth usage will be determined by the outcome of the decision on client access methods, and as such, requirements for the options under consideration have been documented as part of that process. iii. Umoja maintains and has shared with all business and technical stakeholders a detailed list of interfaces planned between SAP, legacy systems, and outside parties. Functional and technical design documents are being drafted for each interface and are subject to the same rigorous approval and testing processes as other development objects. iv. Umoja's anticipated storage requirements

Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
						<p>are documented in the materials supporting the hardware sizing exercise.</p> <p>v. As all production data will be replicated to the disaster recovery site, this volume is documented in the locations mentioned above and will be included in plans for failover support and disaster recovery.</p> <p>vi. The number and nature of licenses required for remote access to SAP is subject to the final disposition of the shared Umoja, OICT, and DFS decisions about client access methods. All relevant scenarios are being documented in support of that decision.</p> <p>Umoja considers that while there is a need to finalize such detailed requirements, initial estimates are available. As such they are able to be updated to reflect the current situation. This is of the ongoing analysis and will be completed/updated/refreshed periodically.</p>
14	The Umoja Office should document the help desk staffing requirements for Umoja production along with escalation procedures	Important	Yes	Team Leader, Technology Solutions	30 April 2013	For issues specifically associated with outages or other incidents related to system availability as reported by end users, notification and escalation procedures related to the Umoja software and hardware infrastructure are being documented by the Umoja technical team and HCL. Umoja is working with OICT and DFS to determine and document analogous procedures for situations related to network incidents. This effort is part of the analysis/work package of the OICT/DFS/Umoja Working Group (A/67/360 paragraph 42 refers).