Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2014/115

Audit of information and communications technology management at the United Nations Office at Geneva

Overall results relating to the effective and efficient management of information and communications technology were initially assessed as partially satisfactory. Implementation of eight important recommendations remains in progress.

FINAL OVERALL RATING: PARTIALLY SATISFACTORY

24 November 2014
Assignment No. AT2014/310/01

CONTENTS

AUDIT REPORT

Audit of information and communications technology management at the United Nations Office at Geneva

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of information and communications technology (ICT) management at the United Nations Office at Geneva (UNOG).

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. UNOG serves as the representative office of the Secretary-General at Geneva, and provides financial and administrative support services to more than 20 Geneva-based United Nations organizations/departments as well as entities located in Bonn and Turin. It manages the United Nations facilities in Geneva and provides conference services for the United Nations meetings held at Geneva as well as for specialized agencies or special arrangements.

4. In accordance with the strategic framework of UNOG for the period 2014-2015, the Information and Communications Technology Service (ICTS) is responsible for ICT operations and, in coordination with the Chief Information Technology Officer (CITO) and the Office of Information and Communications Technology (OICT) of the Department of Management (DM), focuses on the implementation of the Organization's policies on ICT.

5. The ICTS budget for the biennia 2012-2013 and 2014-2015 was $29 million and $28 million, respectively. As of February 2014, ICTS had a complement of 66 staff members.

6. Comments provided by UNOG and DM are incorporated in *italics*.

II. OBJECTIVE AND SCOPE

7. The audit was conducted to assess the adequacy and effectiveness of UNOG governance, risk management and control processes in providing reasonable assurance regarding the **effective and efficient management of ICT at UNOG.**

8. The audit was included in the OIOS 2014 risk-based work plan due to the high risks arising from the dependency of UNOG on ICT systems, and weaknesses in ICT security identified during previous audits.

9. The key controls tested for the audit were: (a) Strategic planning, governance and risk management; (b) Project management capacity; and (c) ICT support systems. For the purpose of this audit, OIOS defined these key controls as follows:

(a) **Strategic planning, governance and risk assessment** – controls that provide reasonable assurance that mechanisms for ICT strategic planning, governance and risk management have been established in UNOG and are working effectively;

(b) **Project management capacity** - controls that provide reasonable assurance that UNOG has appropriate ICT project management capacity to achieve its strategic goals, including: (i) adequate financial resources; (ii) adequate and competent human resources; and (iii) appropriate project management tools, methodology and systems; and

(c) **ICT support systems -** controls that provide reasonable assurance that the ICT systems adequately support the strategic programmes and operations of UNOG.

10. The key controls were assessed for the control objectives shown in Table 1 of the Assessment of key controls table.

11. OIOS conducted this audit from 20 February to 30 April 2014. The audit covered the period from January 2012 to March 2014.

12. 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

13. The UNOG governance, risk management and control processes examined were assessed as **partially satisfactory**[1] in providing reasonable assurance regarding the **effective and efficient management of ICT at UNOG**. OIOS made nine recommendations to address issues identified in the audit. UNOG had established some good control practices with the drafting of a local ICT strategy and the conduct of periodic vulnerability tests. It also received a positive assessment from its user community about the level of ICT support provided to their operations. However, some control weaknesses were identified in the management of ICT, including: (i) inadequate ICT strategic planning and governance mechanisms; (ii) inadequate segregation of ICT duties; (iii) inadequate ICT risk management processes and standard operating procedures; (iv) inconsistent management of ICT projects; (v) inadequate ICT service and change management procedures; (vi) weak pre-implementation activities for the deployment of Umoja – the enterprise resource planning system of the United Nations Secretariat; and (vii) inadequate user access management mechanisms.

14. The initial overall rating was based on the assessment of key controls presented in Table 1 below. The final overall rating is **partially satisfactory** as implementation of eight important recommendations remains in progress.

[1] A rating of **"partially satisfactory"** means that important (but not critical or pervasive) deficiencies exist in governance, risk management or control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

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 and efficient management of ICT at UNOG	(a) Strategic planning, governance and risk assessment	Partially satisfactory	Partially satisfactory	Partially satisfactory	Partially satisfactory
	(b) Project management capacity	Partially satisfactory	Partially satisfactory	Partially satisfactory	Partially satisfactory
	(c) ICT support systems	Partially satisfactory	Partially satisfactory	Partially satisfactory	Partially satisfactory
FINAL OVERALL RATING: PARTIALLY SATISFACTORY					

A. Strategic planning, governance and risk assessment

Inadequate ICT strategy planning processes

An ICT strategy should give direction and establish priorities for the investment and management of resources and a governance framework should define clear roles, responsibilities, criteria and procedures to direct, manage and monitor ICT investments, operations, applications, and infrastructure. In accordance with the Secretary-General's bulletin on "Information and Communications Technology Board", all departments and Offices away from Headquarters shall create internal or local information and communications technology groups or committees and establish departmental strategies aligned with the overall objectives of the Secretariat.

15. As stated in the UNOG strategic framework, ICTS was the main provider of ICT support services. However, several other United Nations entities (i.e., Office of the High Commissioner for Human Rights, Office for the Coordination of Humanitarian Affairs, United Nations Conference on Trade and Development, and Department of Conference Management) operated their own ICT functions. Given that ICTS did not have a clear mandate and authority to determine and enforce the requirements for operating the ICT services of the other United Nations entities hosted in the Geneva complex, UNOG was exposed to significant risks associated with unclear accountabilities, inefficiencies, duplications and, in general, a weak ICT internal control system. In particular:

(i) A review of the Secretary-General's bulletins regulating the ICT operations of UNOG, OHCHR and Economic Commission for Europe showed that the mandate of ICTS for the provision of ICT services in UNOG was defined only with reference to the support of IMIS and related ICT services. Similarly, the responsibility for the provision of ICT services to the other UN entities hosted in the Geneva complex was not defined. Therefore, the lines of authority and communication between ICTS function and some of its clients were not clear;

(ii) The absence of clear mandates to direct ICT operations resulted in services delivered in a fragmented and unregulated manner, often operated in isolation. These limitations were also reflected in the UNOG ICT's draft strategy which stated that UNOG doesn't have a single provider for all its ICT needs;

(iii) There were multiple units providing ICT services with dedicated staff and infrastructures in the Department of Administration of UNOG, including the ICT unit in the Central Support Services (CSS), Human Resources Management Services (HRMS), and Financial Resources Management Service (FRMS);

(iv) Standards for ICT operations and service delivery were not harmonized. There were inconsistent standards for the configuration of information security settings, data centre management, asset management, service management, and infrastructure management;

(v) Business continuity and disaster recovery planning was not adequately coordinated; and

(vi) A central oversight of the UNOG campus-wide ICT projects was not in place.

16. ICTS was in the process of documenting a local ICT strategy. However, there were no strategic planning processes that provided a clear plan and direction for the provision of ICT services in support of UNOG and the other entities hosted in the Geneva complex.

17. Inadequate ICT strategic controls may lead to duplications, misallocation of resources, unnecessary ICT investments, and ICT not focussed on right priorities.

(1) UNOG should, in collaboration with the Department of Management, define its ICT strategy in alignment with the requirements of the Geneva-based United Nations entities.

UNOG accepted recommendation 1 and stated that this recommendation will be implemented based on and in line with the approved global ICT strategy in place in 2015. Recommendation 1 remains open pending receipt of documentary evidence of an ICT strategy that is aligned with the requirements of the Geneva-based United Nations entities.

Lack of an ICT committee

19. The Secretary-General's bulletin on "Information and Communications Technology Board" requires the establishment of local committees to maintain and update information on departmental systems, resources and assets, and ensure the adoption of standard methodologies for ICT projects.

20. UNOG had an ICT Chiefs Committee which functioned as a forum for collaboration and coordination. However, this Committee did not have the mandate and authority to develop ICT strategies and to provide oversight of UNOG ICT systems, resources and assets.

21. The absence of adequate ICT governance structure and mechanisms could lead to unclear roles and responsibilities, and limit the involvement of business users in the definition and assessment of ICT requirements.

(2) UNOG should establish an ICT Steering Committee to review, approve and monitor ICT initiatives.

UNOG accepted recommendation 2 and stated that it will establish an ICT Committee for all entities under the direct authority of the Director-General of UNOG. Subject to issuance of a clear policy directive by the Department of Management, the authority of the ICT Committee would be expanded to include other United Nations Secretariat entities operating in Geneva. Recommendation 2 remains open pending receipt of evidence of the establishment of an ICT

Committee with oversight of all entities of the United Nations Secretariat operating in Geneva.

Misalignment and inadequate segregation of duties in the ICTS organizational structure

22. ICT duties should be segregated so that tasks and associated privileges are assigned to different individuals to ensure adequate checks and balances, and avoid the concentration of full control over an entire process in the hands of one individual.

23. There were cases of ICTS staff performing incompatible tasks, as follows:

(i) In the Solutions Development Unit, one developer worked on all phases of system development, from the definition of requirements to testing, and from migration to production. This condition created potential conflict of interest because it did not allow for an independent review of issues with the accuracy and quality of data or the performance of the applications being developed; and

(ii) In the Infrastructure Management Unit, network administrators were able to configure, administer, and review firewall log activities. This condition created potential conflict of interest because the same staff member could make changes to the security configuration of the network (i.e., changes to the firewall ports) and then delete the logs of his/her own actions.

24. Inadequate segregation of duties may lead to errors or fraud as a result of incompatible job functions being performed by the same person.

(3) UNOG should review the distribution of ICT roles and responsibilities and ensure that a single individual cannot perform incompatible tasks.

UNOG accepted recommendation 3. UNOG subsequently provided OIOS with documentation showing that it had reviewed the distribution of ICT roles and responsibilities and updated its procedures to reduce the risk of a single individual performing incompatible tasks. Based on the action taken by UNOG, recommendation 3 has been closed.

ICT standard operating procedures needed strengthening

25. ICT operations should be managed in accordance with standard operating procedures and policies that ensures repeatable and consistent activities and results that protect ICT operations and assets. Furthermore, there should be a version control mechanism to ensure that only the final and approved version of relevant documents are circulated and implemented.

26. There were some documents detailing the policies and standard operating procedures for ICT operations, asset management, and check-in/check-out. However, the procedure developed by ICTS for "media disposal" was a draft document that was limited to server disks, storage equipment and failed disks. This procedure did not cover important ICT assets such as hard drives of desktops, external storage devices and mobile computing devices. In particular:

(i) Although UNOG had a workflow tool in place for processing check-out actions, the clearance form used by the Human Resources Management Service (HRMS) did not include the requirement to request the termination of access to the ICT applications for the departing staff members. Furthermore, HRMS did not circulate reports of departed staff members to ICTS for ensuring that their access was timely terminated. ICTS relied on the separation notices issued by the individual sections/units to remove access from the active directory;

(ii) ICTS had a documented process for disposing of ICT equipment with recorded data (media disposal procedure). However, this process was primarily related to server disks, storage equipment, and failed disks. Given the fragmentation of asset management within UNOG, this process was not consistently applied across all UNOG entities. Furthermore, there were no mechanisms to determine whether all the computer equipment in UNOG was being disposed of in accordance with the administrative instruction on "Disposal of computer equipment at United Nations Headquarters".; and

(iii) ICTS provided some evidence of the backup procedures designed for the servers of the storage area network. However, complete backup procedures for all other systems were not in place. In particular, the following controls were not defined: (a) backup policies, procedures, and responsibilities; (b) schedules of backups; and (c) classification of data and systems that were required to be backed-up.

27. Inadequate policies and procedures may lead to errors and rework and exposed UNOG to the risk of loss of assets and unauthorized access to ICT systems.

(4) UNOG should design and implement control mechanisms to: (i) ensure that ICT policies and procedures are reviewed on a periodic basis, and are completed with details related to their version and approval; (ii) ensure that changes in the employment status of staff members are communicated to ICTS in a timely manner for regulating their access to ICT systems and applications; (iii) design and implement a procedure to dispose of ICT equipment in a secure manner and in accordance with the requirements established in the administrative instruction on "Disposal of computer equipment at United Nations Headquarters"; and (iv) complete and document the backup procedures for all systems.

UNOG accepted recommendation 4. UNOG subsequently provided additional documentation showing that it had updated existing procedures for the management review of the Information Security Management System. However: (a) there was no consistency in the way the policies were numbered and approved; (b) the separation clearance procedures did not address the need for HRMS to systematically report all separations to ICTS for action; and (c) the Legato Networker Back up procedure did not adequately cover the risk of loss of critical data. Therefore, recommendation 4 remains open pending receipt of evidence showing that: (a) ICT policies and procedures are completed with details related to their version and approval; (b) separation reports are regularly communicated to ICTS for all entities under its purview; (c) all ICT equipment is disposed of in accordance with the applicable administrative instruction; and (d) the back up policy has been updated to establish the criticality of all data held on servers, and the back up actions are documented.

B. Project management capacity

ICT projects were not managed in a consistent manner

28. ICT projects should be managed with a methodology that provides a structured and consistent approach to justify, develop, and approve proposals, define objectives and scope, identify potential risks, and quantify costs and benefits. In this area, the Secretariat documented an ICT project management framework (Projects in a Controlled Environments, PRINCE II) that included procedures for the development, review and approval of ICT initiatives, and governance mechanisms.

29. ICTS had in place a project governance framework that included a Project Management Unit (PMU), project portfolio and a draft document titled "Governance Quick Start for Projects" (GQSP). However, this framework did not apply to ICT initiatives of the other entities hosted in the Geneva complex, and there were no project steering committees to review this process. In addition, the project governance framework adopted by ICTS was not implemented in a consistent manner.

30. The GQSP document developed by ICTS was not aligned with the United Nations Secretariat's project management framework. For example, the Secretariat's framework specified that projects should be classified based on their total cost of ownership. The GQSP document, instead, classified projects by risk levels (high, medium and low), and did not define the scope and boundaries of what should have been included in each risk level. GQSP did not define the change control process for recording, evaluating, and authorizing changes to project scope. These inconsistencies could lead to confusion and prevent a correct monitoring and reporting of the implementation and costs of ICT initiatives across the Secretariat.

(5) UNOG should align its project management framework with that of the United Nations Secretariat.

UNOG accepted recommendation 5. UNOG subsequently provided an updated ICTS project management framework. However, the project management framework did not provide guidance on the preparation of a business case. Recommendation 5 remains open pending receipt of an updated project management framework aligned with the project management framework of the United Nations Secretariat.

Procedures for ICT service management were not adequately documented

31. An ICT service management framework should define the level of support required for the continuous and reliable functioning of ICT operations. The framework should detail criteria and processes to document the requirements of SLA. The framework should also specify roles, tasks, and responsibilities of internal and external service providers and users.

32. ICTS documented a service management framework guide that governed the work of the service management teams. However, the following weaknesses were noted in the processes supporting the ICTS service management framework:

(i) ICTS did not define a service delivery module to reflect its role of central ICT service provider in UNOG;

(ii) ICTS used an automated tool for service desk management, i.e., Open Ticket Request System (OTRS) but did not document criteria, standards, and indicators for monitoring and reporting on service delivery performance;

(iii) ICTS documented a rate card for its various services. However, it did not have a service catalogue describing the services available, with corresponding deliverables, prices, focal points, and processes to request services;

(iv) There were inconsistencies in the use of MoU and SLA to regulate the provision of services to clients. Also, the descriptions of services provided by ICTS in the rate cards were not consistently aligned with the descriptions of services defined in the corresponding MoU/SLA. Hence, clients such as the Division of Conference Management and the Office for Coordination of Humanitarian Affairs could not reconcile the periodic bills with the services received; and

(v) ICTS deployed tools for performance and capacity management that supported various tasks, including: (i) gathering of data; (ii) monitoring performance and capacity on current usage; (iii) determining future capacity requirements for the ICT infrastructure; and (iv) generating reports and statistics on network performance. However, the use of these tools was not supported by pre-defined metrics and baselines to assess performance levels and trends.

33. Inadequate ICT service management may lead to the unavailability of ICT systems and decreased user satisfaction.

(6) UNOG, in collaboration with the Department of Management, should: (i) develop a service delivery model with documented criteria, standards, and performance indicators for ICT service delivery; (ii) review its service catalogue and rate cards to ensure that they provide a complete description of the services available, including details related to deliverables, costs, focal points, and processes for requesting services; (iii) ensure consistency in the establishment of service level agreements and memoranda of understanding to regulate the provision of ICT services to its clients; and (iv) define metrics and baselines for measuring and monitoring the performance of ICT service delivery.

UNOG accepted recommendation 6 and stated that it will meet the recommendation in consultation with service management specialists within DM. Recommendation 6 remains open pending receipt of documentation showing: (i) the implementation of a service delivery model, service catalogue, and rate cards, consistently applied in the SLA and MoU regulating the provision of ICT services in UNOG; and (ii) the development of metrics and baselines for measuring and monitoring ICT service delivery in UNOG.

Change management procedures were not adequate

34. A change management procedure should include control mechanisms to ensure that changes to the ICT infrastructure and applications, including emergency maintenance and patches, are adequately reviewed, approved, monitored and reported. Changes should be logged, assessed and authorized prior to their implementation.

35. Although, ICTS documented a change management policy, controls were not in place to ensure that all the changes to ICT infrastructure and applications were controlled. Change requests were not consistently logged in UNOG with the risk of disregarding critical systemic issues and the root-cause of potential problems affecting the ICT operations of the Office. In particular, the following weaknesses were noted:

(i) Not all the requests for changes were logged in the central database. ICTS had multiple tools in place to log requests for changes. The requests for changes submitted by the clients directly to the Solutions Development Unit were not logged in a consistent manner in the OTRS system; and

(ii) Although, the change management policy identified incident management as an entry point for change, at the operational level this control was not performed when an incident required a request for change to be logged. There was no alignment between the incident management logs kept by the Infrastructure Management Unit and the data recorded in the central database.

36. The absence of a centralized database for managing and monitoring change requests may have a negative impact on the continuity and security of ICT operations, and potentially lead to errors or loss of data.

(7) UNOG should ensure that all ICT change requests, including those derived from incidents, are controlled and logged in one central database.

UNOG accepted recommendation 7. UNOG subsequently provided documentation showing that it had updated its change management policy by establishing iNeed as the central database for all ICT change requests. However, UNOG did not provide evidence showing that it had started using iNeed for all ICT change requests. Recommendation 7 remains open pending receipt of documentation showing that UNOG is using iNeed for logging all ICT change requests.

C. ICT support systems

Pre-implementation activities for the deployment of Umoja needed strengthening

37. The deployment of Umoja in UNOG is scheduled for June 2015. In preparation for the deployment, it is necessary for UNOG to have clear terms of reference to ensure that adequate actions are taken in preparation for the deployment.

38. In February 2014, UNOG received from the Umoja Office a deployment plan for the implementation of the new system (Umoja Deployment Guide), and had a dedicated officer responsible for coordinating project activities. However, UNOG was of the view that the guidance received from the Umoja Office was not actionable because it lacked adequate details to determine the ICT resources and actions required for preparing for the implementation of Umoja.

39. Inadequate definition of the ICT resources and actions needed in preparation for the implementation of Umoja could lead to delays in its deployment.

(8) UNOG should request the Department of Management to define the actions required for the preparation to implement Umoja in Geneva in a timely manner.

UNOG accepted recommendation 8. UNOG subsequently provided a memorandum it had written to OICT, as well as the response received from OICT. These memoranda indicated that UNOG participated in the monthly Umoja steering committee meetings and the weekly ICT Umoja deployment readiness meetings facilitated by OICT, and OICT had also requested its focal point for the Umoja project to review in detail all the ICT tasks in the Umoja Cluster 3 scorecard to ensure clarity and help to define specific action items for UNOG. Recommendation 8 remains open pending receipt of the specific action items defined by DM for preparation to implement Umoja in Geneva.

Inadequate user access management mechanisms

40. User access to systems and applications should be controlled with procedures and mechanisms for requesting, granting, suspending, modifying and terminating access and related privileges. These procedures should apply to all users, for both standard and emergency cases.

41. ICTS did not have policies and procedures for managing user access to systems and applications. Given the composition of UNOG, ICTS did not have adequate authority to manage access requests issued by all the clients serviced. Also, ICTS had not implemented adequate mechanisms for monitoring the use of privileged access, and managing them with adequate segregation of duties (i.e., network administrator). Although, there were some documents supporting the management of the Windows active

directory (i.e., for the domain controller audit policy and the active directory account creation), these documents contained several weaknesses.

42. The absence of an adequate mechanism for managing user access to systems may lead to unauthorized access and loss of confidential information.

(9) UNOG should develop and implement an access control policy that includes criteria for: (i) granting privileged access; and (ii) conducting regular reviews of user access to all ICT systems.

UNOG accepted recommendation 9. UNOG subsequently provided documentation showing that it had finalized the ICTS access control policy which included a specific process flow to manage requests for privileged access. However, UNOG did not provide evidence of conducting a review of user access to all ICT systems. Recommendation 9 remains open pending receipt of evidence showing that UNOG regularly reviews user access to all its ICT systems.

IV. ACKNOWLEDGEMENT

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

(*Signed*) David Kanja
Assistant Secretary-General for Internal Oversight Services

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of information and communications technology management at the United Nations Office at Geneva

Recom. no.	Recommendation	Critical[2]/ Important[3]	C/ O[4]	Actions needed to close recommendation	Implementation date[5]
1	UNOG should, in collaboration with the Department of Management, define its ICT strategy in alignment with the requirements of the Geneva-based United Nations entities.	Important	O	Receipt of documentary evidence of an ICT strategy that is aligned with the requirements of the Geneva-based United Nations entities.	31 December 2015
2	UNOG should establish an ICT Steering Committee to review, approve and monitor ICT initiatives.	Important	O	Receipt of evidence of the establishment of an ICT Committee with oversight of all entities of the United Nations Secretariat operating in Geneva.	31 March 2015
3	UNOG should review the distribution of ICT roles and responsibilities and ensure that a single individual cannot perform incompatible tasks.	Important	C	Action completed.	Implemented.
4	UNOG should design and implement control mechanisms to: (i) ensure that ICT policies and procedures are reviewed on a periodic basis, and are completed with details related to their version and approval; (ii) ensure that changes in the employment status of staff members are communicated to ICTS in a timely manner for regulating their access to ICT systems and applications; (iii) design and implement a procedure to dispose of ICT equipment in a secure manner and in accordance with the requirements established in the administrative instruction on "Disposal of computer equipment at United Nations Headquarters"; and (iv) complete and document the backup procedures for all systems.	Important	O	Receipt of evidence showing that: (a) ICT policies and procedures are completed with details related to their version and approval; (b) separation reports are regularly communicated to ICTS for all entities under its purview; (c) all ICT equipment is disposed of in accordance with the applicable administrative instruction; and (d) the back up policy has been updated to establish the criticality of all data held on servers, and the back up actions are documented.	31 December 2014

[2] 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.
[3] 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.
[4] C = closed, O = open
[5] Date provided by UNOG in response to recommendations.

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of information and communications technology management at the United Nations Office at Geneva

Recom. no.	Recommendation	Critical[2]/ Important[3]	C/ O[4]	Actions needed to close recommendation	Implementation date[5]
5	UNOG should align its project management framework with that of the United Nations Secretariat.	Important	O	Receipt of an updated project management framework aligned with the project management framework of the United Nations Secretariat.	31 December 2014
6	UNOG should, in collaboration with the Department of Management, should: (i) develop a service delivery model with documented criteria, standards, and performance indicators for ICT service delivery; (ii) review its service catalogue and rate cards to ensure that they provide a complete description of the services available, including details related to deliverables, costs, focal points, and processes for requesting services; (iii) ensure consistency in the establishment of service level agreements and memoranda of understanding to regulate the provision of ICT services to its clients; and (iv) define metrics and baselines for measuring and monitoring the performance of ICT service delivery.	Important	O	Receipt of documentation showing: (i) the implementation of a service delivery model, service catalogue, and rate cards, consistently applied in the SLA and MoU regulating the provision of ICT services in UNOG; and (ii) the development of metrics and baselines for measuring and monitoring ICT service delivery in UNOG	31 December 2015
7	UNOG should ensure that all ICT change requests, including those derived from incidents, are controlled and logged in one central database.	Important	O	Receipt of documentation showing that UNOG is using iNeed for logging all ICT change requests.	31 December 2014
8	UNOG should request the Department of Management to define the actions required for the preparation to implement Umoja in Geneva in a timely manner.	Important	O	Receipt of the specific action items defined by DM for preparation to implement Umoja in Geneva.	31 December 2014
9	UNOG should develop and implement an access control policy that includes criteria for: (i) granting privileged access; and (ii) conducting regular reviews of user access to all ICT systems.	Important	O	Receipt of evidence showing that UNOG regularly reviews user access to all its ICT systems.	31 December 2014

APPENDIX I

Management Response

Office des Nations Unies à Genève United Nations Office in Geneva

MEMORANDUM INTERIEUR INTEROFFICE MEMORANDUM

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

DATE: 17 October, 2014

REF.

FROM: Clemens M. Adams
DE: Director
Division of Administration, UNOG

SUBJECT: **Draft report on an audit of information and communications technology management at the United Nations Office at Geneva**
OBJET: **(Assignment No.AT2014/310/01)**

---

1. Please refer to my memorandum dated of 23 September 2014 pertaining to the above subject.

2. Attached please the duly completed management response form, Appendix I, which has been finalized following consultations with relevant offices of the Department of Management.

3. UNOG has proactively worked on addressing all issues identified in the report. To this end 17 pieces of evidence were sent to the audit team in the past days. In our view these provide evidence that recommendations 3, 4, 5, 7, 8 and 9 have been effectively addressed by UNOG. We stand ready to provide further evidence in this regard should this be required to complete the audit process for these recommendations.

4. In view of the above, may I kindly request that these additional elements be taken into account when preparing the final audit.

5. Let me take this opportunity to express our appreciation for your understanding and support in this important matter.

Cc: Mr. Zachary Ikiara, Chief, Oversight and Coordination Support Unit, DM
Ms. Cynthia Avena-Castillo, Professional Practices Section, Internal Audit Division, OIOS
Mr. Anthony O'Mullane, Director, OICT
Mr. Eric Chan, Compliance Officer, OICT
Mr. Luis Santiago, Chief, ICTS, Division of Administration, UNOG

APPENDIX I

Management Response

Audit of information and communications technology management at the United Nations Office at Geneva

Rec. no.	Recommendation	Critical/ Important	Accepted? (Yes/No)	Title of responsible individual	Implementation Date	Client comments
1	UNOG should, in collaboration with the Department of Management, define its ICT strategy in alignment with the requirements of the Geneva-based United Nations entities.		Yes	Director General, UNOG	31-Dec-2015	This recommendation will be implemented based on and in line with the approved global ICT strategy in place at that time in 2015.
2	UNOG should establish an ICT Steering Committee to review, approve and monitor ICT initiatives.		Yes	Director General, UNOG	31-Mar-2015	UNOG will establish an ICT Committee for all entities under its direct authority of the DG UNOG. Subject to issuance of a clear policy directive by DM the authority of the ICT Steering Committee would be expanded to include other UN Secretariat entities operating in Geneva.
3	UNOG should review the distribution of ICT roles and responsibilities and ensure that a single individual cannot perform incompatible tasks.		Yes	Chief, ICTS, Division of Administration, UNOG	31-Dec-2014	

APPENDIX I

Management Response

Audit of information and communications technology management at the United Nations Office at Geneva

Rec. no.	Recommendation	Critical/ Important	Accepted? (Yes/No)	Title of responsible individual	Implementation Date	Client comments
4	UNOG should design and implement control mechanisms to: (i) ensure that ICT policies and procedures are reviewed on a periodic basis, and are completed with details related to their version and approval; (ii) ensure that changes in the employment status of staff members are communicated to ICTS in a timely manner for regulating their access to ICT systems and applications; (iii) design and implement a procedure to dispose of ICT equipment in a secure manner and in accordance with the requirements established in the administrative instruction on "Disposal of computer equipment at United Nations Headquarters"; and (iv) complete and document the backup procedures for all systems.		Yes	Chief, ICTS, Division of Administration, UNOG	31-Dec-2014	
5	UNOG should align its project management framework with that of the United Nations Secretariat.		Yes	Chief, ICTS, Division of Administration, UNOG	31-Dec-2014	

APPENDIX I

Management Response

Audit of information and communications technology management at the United Nations Office at Geneva

Rec. no.	Recommendation	Critical/ Important	Accepted? (Yes/No)	Title of responsible individual	Implementation Date	Client comments
6	UNOG should, in collaboration with the Department of Management: (i) develop a service delivery model with documented criteria, standards, and performance indicators for ICT service delivery; (ii) review its service catalogue and rate cards to ensure that they provide a complete description of the services available, including details related to deliverables, costs, focal points, and processes for requesting services; (iii) ensure consistency in the establishment of service level agreements and memoranda of understanding to regulate the provision of ICT services to its clients; and (iv) define metrics and baselines for measuring and monitoring the performance of ICT service delivery.		Yes, with caveats	Chief, ICTS, Division of Administration, UNOG	31-Dec-2015	UNOG to meet recommendation in consultation with Service Management specialists within DM. Caveats: for some of the required points OIOS is not applying required UN policy but bodies of best practices in general not required by the UN; given that no additional budget for said potentially resource intensive processes has been allotted, on points (i) and (iv), UNOG will scope the implementation so it reasonably provides the requested elements within the limits of existing resources, by using its own managerial discretion with regards to what performance indicators, monitoring, metrics and measurements can be defined and sustained.
7	UNOG should ensure that all ICT change requests, including those derived from incidents, are controlled and logged in one central database.		Yes	Chief, ICTS, Division of Administration, UNOG	31-Dec-2014	
8	UNOG should request the Department of Management to define the actions required for the preparation to implement Umoja in Geneva in a timely manner.		Yes	Chief, ICTS, Division of Administration, UNOG	31-Dec-2014	

APPENDIX I

Management Response

Audit of information and communications technology management at the United Nations Office at Geneva

Rec. no.	Recommendation	Critical/ Important	Accepted? (Yes/No)	Title of responsible individual	Implementation Date	Client comments
9	UNOG should develop and implement an access control policy that includes criteria for: (i) granting privileged access; and (ii) conducting regular reviews of user access to all ICT systems.		Yes	Chief, ICTS, Division of Administration, UNOG	31-Dec-2014	