



OIOS

Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

AUDIT REPORT

ICT systems supporting the Capital Master Plan

The CMP office needs to establish a strategic and governance framework that ensures the security, integration and oversight of ICT processes and assets

18 September 2009

Assignment No. AT2008/514/01

United Nations  Nations Unies

INTEROFFICE MEMORANDUM

MEMORANDUM INTERIEUR

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

TO: Ms. Angela Kane, Under-Secretary-General
A: Department of Management

DATE: 18 September 2009

Mr. Michael Adlerstein
Assistant Secretary-General and Executive Director,
Capital Master Plan

REFERENCE: IAD: 09-02888

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



SUBJECT: **Assignment No. AT2008/514/01 - Audit of ICT systems supporting the Capital Master Plan**

OBJET:

The CMP office needs to establish an ICT strategic and governance framework that ensures the security, integration and oversight of ICT processes and assets.

1. I am pleased to present the report on the above-mentioned audit.
2. In order for us to close the recommendations, we request that you provide us with the additional information as discussed in the text of the report and also summarized in Annex 1.
3. Please note that OIOS will report on the progress made to implement its recommendations, particularly those designated as high risk (i.e., recommendations 7, 9 & 10), in its annual report to the General Assembly and semi-annual report to the Secretary-General.

cc: Mr. Soon-hong Choi, Assistant Secretary-General, OICT
Mr. Swatantra Goolsarran, Executive Secretary, UN Board of Auditors
Ms. Suzanne Frueh, Executive Secretary, Joint Inspection Unit
Mr. Moses Bamuwamye, Chief, Oversight Support Unit, Department of Management
Mr. Byung-Kun Min, Special Assistant to the USG-OIOS
Mr. William Petersen, Chief, New York Audit Service, OIOS

INTERNAL AUDIT DIVISION

FUNCTION

"The Office shall, in accordance with the relevant provisions of the Financial Regulations and Rules of the United Nations examine, review and appraise the use of financial resources of the United Nations in order to guarantee the implementation of programmes and legislative mandates, ascertain compliance of programme managers with the financial and administrative regulations and rules, as well as with the approved recommendations of external oversight bodies, undertake management audits, reviews and surveys to improve the structure of the Organization and its responsiveness to the requirements of programmes and legislative mandates, and monitor the effectiveness of the systems of internal control of the Organization" (General Assembly Resolution 48/218 B).

CONTACT INFORMATION

ACTING DIRECTOR:

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

CHIEF, NEW YORK AUDIT SERVICE:

William Petersen: Tel: +1.212.963.3705, Fax: +1.212.963.3388,
e-mail: petersenw@un.org

EXECUTIVE SUMMARY

Audit of ICT systems supporting the Capital Master Plan

OIOS conducted an audit of the information and communications technology (ICT) systems supporting the Capital Master Plan (CMP). The overall objective of the audit was to assess the adequacy of the controls established to ensure the secure, efficient and effective operations of the ICT systems. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

CMP had a basic ICT infrastructure and used a website as a communication tool providing up-to-date information to all stakeholders on the current status of the project.

OIOS noted that CMP had established positive joint working arrangements with the Office of Programme Planning, Budget and Accounts (OPPBA), for the adoption of the NOVA system to support the CMP's internal information processing. However, several control weaknesses are still preventing CMP from obtaining an adequate ICT infrastructure to support its operations in a secure, efficient and effective manner including:

- (i) Lack of an ICT strategic and governance framework to define and manage the information needs of the CMP project;
- (ii) Lack of a defined ICT infrastructure in support of the CMP project;
- (iii) Lack of documented information security procedures to protect data and systems;
- (iv) Lack of non-disclosure agreements with third party contractors accessing UN data and information;
- (v) Lack of documented procedures for monitoring and internal controls;
- (vi) Inconsistencies in business continuity planning and backup procedures;
- (vii) Lack of documented procedures for ICT acquisition, implementation and change management; and
- (viii) Lack of oversight and control over UN data/information processed and held by third party contractors.

TABLE OF CONTENTS

Chapter	Paragraphs
I. INTRODUCTION	1-9
II. AUDIT OBJECTIVES	10
III. AUDIT SCOPE AND METHODOLOGY	11-14
IV. AUDIT FINDINGS AND RECOMMENDATIONS	
A. Strategy & governance	15-20
B. Infrastructure	21-28
C. Security and data integrity	29-38
D. Disaster recovery & business continuity	39-42
E. Managing ICT investments	43-46
F. UN data managed by third parties	46-51
V. ACKNOWLEDGEMENT	52
ANNEX 1 – Status of audit recommendations	

I. INTRODUCTION

1. The Office of Internal Oversight Services (OIOS) conducted an audit of information and communications and technology (ICT) systems supporting the Capital Master Plan (CMP). The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

2. The CMP project is a capital renovation project of UNHQ. The project has a current budget of \$1,876.7 million, which was approved by the General Assembly with resolution 61/251 on 22 December 2006. Renovation work is expected to be completed by 2013.

3. Decision-making in the construction industry is driven by the need to overcome project uncertainties and adequately manage internal and external interdependencies. These requirements make it imperative for constant availability of data, and reliable and effective technologies to enable effective decision-making.

4. Information management and data processing for the CMP project was performed both internally and externally. Allotment, expenditure and disbursement processing was undertaken using existing UN systems and procedures.

Name of system	Source	Purpose
NOVA	Internal	Workflow
Quick place FTP	Internal	Secure shared workspace
Team site	External	Integrated repository for sharing documents and information
Primavera	External	Project planning
IMIS	Internal	Accounting, payments

5. As the CMP project evolved, it was determined that the existing main financial system of the United Nations Secretariat – the Integrated Management Information System (IMIS) was not going to be able to address the data management requirements of the project. The nature of these requirements demanded the processing of granular financial information for budgeting and reporting.

6. The CMP office identified the need for a centralized repository of data, and comprehensive access to information that related to the overall budget, project phases, contracts, obligations (either under preparation or approved) and payments. These needs have been addressed with the adoption of NOVA.

7. NOVA was originally developed and used by OPPBA. To enable its use in the CMP environment, a module of the application was customized specifically for CMP. While NOVA served as a workflow system for entering CMP financial information into IMIS, the latter provided the financial and management accounting tool to enable the project.

8. In addition, CMP adopted other purpose-specific systems owned and managed by third party contractors.

9. Comments made by the Office of the Capital Master Plan are shown in *italics*.

II. AUDIT OBJECTIVES

10. The main objectives of the audit were to assess whether:

- (a) CMP was adequately supported by ICT systems;
- (b) The ICT systems were effectively and efficiently governed; and
- (c) Effective general controls existed over:
 - (i) Security;
 - (ii) Access controls;
 - (iii) Program and data changes;
 - (iv) Segregation of duties; and
 - (v) Service continuity.

III. AUDIT SCOPE AND METHODOLOGY

11. The audit included a review of policies, standard operating procedures, and guidelines to assess the ICT governance and security operating environment.

12. In addition, questionnaires were issued to key officers to obtain background information.

13. Interviews were held with representatives from CMP, OPPBA, OICT, and the third party contractors Skanska, Gardiner & Theobold (G&T) and Kroll.

14. Tests were performed on key systems to confirm the adequacy of controls, as well as to identify threats, risks and vulnerabilities that may affect the integrity and security of data.

IV. AUDIT FINDINGS AND RECOMMENDATIONS

A. Strategy and governance

Lack of an effective ICT strategic and governance framework to define and manage the information needs of the CMP project

15. The development of an ICT strategic and governance framework is essential to ensure the effective and efficient use of information technologies in line with the objectives of the CMP project. CMP did not define its ICT needs in terms of data, technology and systems to support the project. It also lacked an effective ICT governance body and mechanisms to ensure that ICT systems and processes were aligned with the objectives of the project and best practice.

16. The strategic and operational accountability for information management in the context of the CMP project rests with the Assistant Secretary-General (ASG) for CMP. However, operational responsibilities for ICT, including the administration and security of information, had not been formally assigned to any officer within CMP. Although the CMP office had an ICT support post within OICT (formally ITSD), there was no evidence that the duties performed by the incumbent adequately addressed the ICT needs of the project. In particular, oversight criteria were not clearly defined for the following critical control areas:

- (a) Data and information requirements of the CMP project;
- (b) ICT expenditure related to CMP;
- (c) Security of ICT assets and data; and
- (d) Policies and standard operating procedures.

17. In addition, CMP lacked a formal risk assessment process and did not review the applications and systems in use to ensure that risks were identified, assessed and mitigated by effective controls.

Recommendations 1 to 3

The Office of the Capital Master Plan should:

- (1) Establish an ICT working group/committee to review, approve, and oversee all ICT initiatives;**
- (2) Formally assign clear responsibilities to an officer, to ensure adequate administration and support of the ICT function; and**
- (3) Perform a risk assessment of all ICT systems supporting CMP, to identify risks and mitigating controls.**

18. *The Office of the Capital Master Plan accepted recommendation 1 and stated that CMP participates in the DM ICT Committee, which was recently reconstituted.* Recommendation 1 remains open pending receipt of the formal terms of reference for the reconstituted DM ICT Committee, detailing the oversight function over the ICT systems of the CMP project.

19. *The Office of the Capital Master Plan accepted recommendation 2 and stated that it has an ICT focal point at the GS level that supports the administration of the ICT function.* In OIOS' view, the complexity of the ICT systems supporting the CMP project requires a professional level of technical competence and expertise. Therefore, recommendation 2 remains open pending the assignment of the responsibilities for the support of the ICT systems to a professional staff member.

20. *The Office of the Capital Master Plan accepted recommendation 3 and stated that in context of the pandemic preparedness, critical systems and functions were identified, and mitigating measures for uninterrupted access put in place (through CITRIX).* Recommendation 3 remains open pending receipt by OIOS of the documented analysis conducted by CMP for the identification of the critical systems and the definition and implementation of the mitigating measures.

B. Infrastructure

Lack of a defined ICT infrastructure in support of the CMP project

21. Best practices recommend that organizations develop structured and documented information models to ensure adequate integration of systems and applications, as well as their cost-effectiveness, security and compliance with internal requirements. Since CMP had not documented an information model, its systems had evolved in a piecemeal manner through the use of both in-house developed applications and externally acquired software.

22. CMP lacked a framework to ensure the effective integration of ICT systems, in particular between its in-house developed applications and those provided and used by third party contractors. OIOS identified five application systems that supported the CMP project, with some instances of duplicated functionalities among them. There was no operational integration of these systems and no central oversight to ensure the security and integrity of the data contained within these applications. In addition, operational and functional responsibilities were distributed among several staff.

23. To support the effective use of information and better collaboration between stakeholders, it is a good practice to have a central repository of structured data. CMP did not have a dedicated system for supporting the structured creation, capture, storage and dissemination of information. Internally, reliance was placed on the shared drive as a central repository of documents. Since the taxonomy of the shared drive was not documented, it was difficult for users to locate information. In addition, two other applications managed by external contractors were also used to share and communicate information. The

lack of one integrated system limited the effective and efficient sharing of information among staff, and prevented an adequate version control of documents. However, OIOS acknowledged the pending implementation of the Corporate Electronic Content Management system (ECM), which will provide a standard environment and tools for the creation, capturing, storing and dissemination of information. Since this system is currently being developed within the United Nations Secretariat, OIOS is not issuing a recommendation on this matter.

Lack of adequate service level agreements

24. The provision of adequate service to the ICT systems used by CMP were limited by two main control weaknesses:

- (a) The SLA established in 2007 between CMP and OPPBA for the support of the NOVA system had not been updated since then; and
- (b) No SLA was in place between CMP and OICT for the maintenance of CMP applications.

25. This condition exposed CMP to the risk of untimely maintenance actions and delays in the resolution of problems with the performance of its ICT systems.

Recommendations 4 to 6

The Office of the Capital Master Plan should:

- (4) Develop and implement an ICT model that facilitates the optimal creation, use and sharing of information between staff members;**
- (5) Document an information module integrating both internal and external ICT applications to ensure effective systems operation, reliability and integrity of data, and continuity or recovery of operations in the event of a disaster; and**
- (6) Update internal service level agreements with OICT and OPPBA for the support of all CMP systems. These agreements should include: service desk requests to process problems/errors; monitoring of requests against established internal service level agreements; and call escalation procedures.**

26. *The Office of the Capital Master Plan accepted recommendation 4 and stated that CMP relies on UN corporate standards established by OICT for information sharing between staff members. Recommendation 4 remains open pending the development and creation by CMP of an ICT model, in accordance with the UN standards established by OICT for information sharing.*

27. *The Office of the Capital Master Plan accepted recommendation 5 and stated that they rely entirely on OICT and UN corporate standards for operations, reliability, continuity of operations and disaster recovery. Recommendation 5 remains open pending documentation of an information module integrating both internal and external ICT providers to ensure effective systems operation, reliability and integrity of data, and continuity of operations in the event of a disaster or recovery.*

28. *The Office of the Capital Master Plan accepted recommendation 6 and stated that they have a SLA with Office of Information Communication and Technology for corporate systems support, and a written agreement with FIOS with regard to NOVA. They also have a separate maintenance contract with NOVA with an outside consultant. The SLA provided to OIOS for the NOVA application was outdated. In addition, no SLA was provided to OIOS for the other applications used by CMP, such as Quickplace, and the CMP website. Therefore, recommendation 6 remains open pending the update of internal service level agreements established by CMP with OICT and OPPBA for the support of all CMP systems. These agreements should include service desk procedures to process problems/errors; monitoring of requests against established internal service level agreements; and call escalation procedures.*

C. Security and data integrity

Lack of documented information security procedures to protect data and systems

29. Proper management of information security is essential for ensuring the protection of ICT assets, critical information, and the integrity of data. There was limited evidence that CMP had formally considered information security controls as part of its control environment. CMP had not defined or documented its information security procedures for internal use, and for the third party contractors with direct access to UN ICT resources and information. Also, CMP had not assigned responsibilities for the management and security of information. This condition exposed CMP to risks of breaches of confidentiality, and loss or unavailability of data.

Recommendations 7 and 8

The Office of the Capital Master Plan should:

(7) Document information security procedures, and assign responsibilities for the management and enforcement of security procedures; and

(8) Use the CMP website to undertake regular information security awareness sessions and to remind all stakeholders of the need to safeguard CMP information resources.

30. *The Office of the Capital Master Plan accepted recommendation 7 and stated that information security requirements are incorporated into the contracts*

with the relevant firms, and further implemented through the use of passwords and limited access to applications (as facilitated by OICT). Recommendation 7 remains open pending receipt of documentation of the CMP information security procedures.

31. *The Office of the Capital Master Plan accepted recommendation 8 and stated it will remind all stakeholders of the need to safeguard CMP information resources. The CMP added that it will also communicate the importance of this matter in the quarterly principals meetings. Recommendation 8 remains open pending receipt by OIOS of documentation showing that security awareness initiatives have been undertaken by CMP.*

Lack of non-disclosure agreements with third party contractors

32. CMP did not have standard information management and security provisions as part of its contracts with third party contractors who had access to UN data and information. Vendors' contracts included a clause on confidentiality and intellectual property rights but did not define the responsibilities and accountability for the management and security of information handled by third parties. By not establishing information security agreements with third party contractors, CMP risked breaches to the confidentiality, integrity and availability of CMP data and information.

Lack of documented monitoring and internal controls

33. Access control procedures should exist to control and manage system application rights and privileges, in accordance with the organisation's security policies. CMP did not define and document data access and monitoring rules for access to systems (both by internal and external users) containing UN data or information. This condition exposed CMP data to the risk of breaches of confidentiality and data loss.

34. OIOS obtained a user access list of three of the main CMP systems (NOVA, Quickplace and Primavera), and conducted an analysis to confirm the adequacy of their security and integrity controls. The following weaknesses were identified:

(a) Cases whereby duties were not adequately segregated. Two officers were identified in the NOVA system as both administrators and users, and one user in the Quickplace application had conflicting profiles of "manager" and "author", giving the users the ability to perform unauthorised transactions without detection;

(b) User access was not monitored for non-activity and access breaches e.g. there were five out of 33 users that had not signed in the system for more than 6 months and two users that had never logged on.

(c) Both the NOVA and Quickplace users' lists included staff who were no longer employed within the UN;

(d) Access logs for monitoring purposes were not readily available for the Quickplace application;

(e) Access to third party systems were sometimes granted on the basis of oral communication without any documented request or authorisation; and

(f) A user had two profiles (two system manager profiles) on the Quickplace application.

35. Primavera is a scheduling application owned and used by the contractor (G&T). OIOS noted that a user profile enabled in the system (project scheduler) could also act as administrator of the application, controlling access and security parameters of the system, thus negating adequate segregation of duties.

Recommendation 9

(9) The Office of the Capital Master Plan should document data access rules and requirements for all ICT systems supporting CMP and ensure they are applied to all users of the systems, including third party contractors.

36. *The Office of the Capital Master Plan accepted recommendation 9 and stated that it mostly uses UN standard software and applications, and access is given on a case by case basis. As for Nova, CMP has defined four different user roles and access levels, and these roles are applied on a need basis.* Recommendation 9 remains open pending the receipt of documented data access rules and requirements for all users (both internal and external) of the ICT systems supporting CMP.

Data integrity

37. OIOS identified that the automatic transfer of data between the two main information systems (IMIS and NOVA) used by CMP was unidirectional. While data was automatically transferred between IMIS to NOVA, the reverse flow from NOVA to IMIS was based on manual input. In order to ensure the reliability of data, CMP staff periodically reconciled information between the two systems, identifying missing batches, and issuing email requests to OPPBA for updates.

38. CMP requested modifications to the NOVA system to automate the processes for reviewing, clearing, certifying, categorising and monitoring data. However, in consideration of the pending implementation of the ERP system at the United Nations Secretariat, the costs and use of resources required for the completion of these changes could not be justified. OIOS is of the opinion that the need for manual input of data negates the efficiency of an automated workflow process. However, acknowledging that the ERP system will provide adequate data integration, at this time, OIOS is not issuing a recommendation as regards this matter.

D. Disaster recovery & business continuity

Inconsistencies in business continuity planning and backup procedures

39. Business continuity procedures should specify information and requirements pertaining to: (a) organizational structure for continuity management; (b) roles; (c) tasks; (d) responsibilities of internal and external service providers; (e) rules for documenting, executing, and testing disaster recovery procedures; and (f) ICT contingency plans. OIOS noted that with the exception of the NOVA system, there was no evidence that the other systems supporting the CMP project have been included in the business continuity and disaster recovery plans of the United Nations Secretariat. Furthermore, CMP had not assessed the adequacy of the disaster recovery plans and backup procedures of third party contractors to ensure the timely availability and recovery of UN data stored by them, in case of an emergency or disaster.

40. A business impact analysis of ICT systems supporting CMP is critical to the identification of potential risks, and the estimation of the impact that the CMP project could suffer should an adverse event occur. CMP did not perform a project impact analysis of its ICT systems. The lack of this analysis could result in difficulties in ensuring the availability of critical ICT resources, increased costs for continuity management and inadequate prioritization of service recovery.

Recommendations 10 and 11

The Office of the Capital Master Plan should:

(10) Document backup and disaster recovery procedures for all ICT systems supporting CMP, and develop a process for coordinating the disaster recovery plans of both internal and external users; and

(11) Conduct a business impact analysis of all ICT systems supporting CMP.

41. *The Office of the Capital Master Plan accepted recommendation 10 and stated that it relies entirely on OICT support in this area, since CMP does not have the expertise or resources to perform this function. CMP is of the opinion that OICT, being the main service provider for ICT, should be consulted for this matter. CMP will write to OICT to communicate this audit observation and seek confirmation that such procedures are in place. Recommendation 10 remains open pending receipt of confirmation from OICT that backup and disaster recovery procedures cover all ICT systems that support CMP, including those provided by third party contractors.*

42. *The Office of the Capital Master Plan accepted recommendation 11 and stated that it uses standard systems and software in use across the UN. In the context of the pandemic preparedness, critical applications have been identified and key staff has already been given remote access via CITRIX.*

Recommendation 11 remains open pending receipt of documentation showing that a business impact analysis of all ICT systems supporting CMP has been conducted.

E. Managing ICT investments

Lack of documented procedures for ICT acquisition, implementation, and change management

43. The ICT systems supporting CMP evolved over the life of the project, without a formal change management process for ICT applications, systems, and services. CMP also lacked a project management framework, and did not have an internal forum/body representative of all stakeholders to manage and oversee ICT initiatives, such as the one related to the request for modifications and enhancements of the NOVA system. In particular, this initiative did not include: i) specific user requirements; ii) a formal process for the approval of the changes or amendments; and iii) a sign off process.

Recommendations 12 and 13

The Office of the Capital Master Plan should:

(12) Define a standard methodology to prepare, review, and approve ICT projects and initiatives, and introduce a cost-benefit analysis for ICT projects and initiatives; and

(13) Document change management procedures and user acceptance test procedures to ensure that: (a) requirements are recorded and tracked even when rejected; (b) changes are recorded during the complete life-cycle of design, development and implementation phases; and (c) acceptance and approval are adequately documented.

44. *The Office of the Capital Master Plan accepted recommendation 12 and stated that CMP uses mainly corporate UN applications. Where small ICT projects have been undertaken in the past, a consistent methodology was used whereby a proposal was submitted to the Executive Director for decision-making. OIOS acknowledges the procedures followed by CMP for small scale projects, but noted that this was not evident during the audit and neither was the process documented for reference. Therefore, recommendation 12 remains open pending receipt of documented procedures for the management of ICT projects commissioned by CMP.*

45. *The Office of the Capital Master Plan accepted recommendation 13 and stated that in most cases they rely on standard UN applications. In the past, where applicable, the management of changes involving testing and acceptance was documented in emails (which they considered adequate given the small size of the projects.) OIOS acknowledges the procedures followed by CMP but noted that this was not evident during the audit and neither was the process documented*

for reference. Recommendation 13 remains open pending receipt of evidence documenting the changes approved and implemented in the ICT systems in use at CMP.

F. UN data managed by third parties

Lack of oversight and control over UN data and information processed and held by third party contractors

46. An application (Team site) owned by the contractor Skanska was used as a repository for information and as a means to share issues that required action between Skanska, CMP and other stakeholders (i.e G&T). OIOS noted that when users posted items requiring follow-up actions into this application the recipient was not automatically alerted to the communication and risked delayed actions. Skanska explained that the software had workflow features which could alert recipient about the creation of communications. However, this feature was not enabled in the current configuration of the system used by CMP.

47. UN data stored in the Skanska's system was maintained on servers physically located in the Skanska's office in North Carolina. In this regard, OIOS determined that CMP had not conducted, nor requested, a security assessment confirming the adequacy of Skanska's information security controls, backup procedures and disaster recovery arrangements to provide assurance as to the availability, security and integrity of UN data.

48. The CMP Quickplace system is a UN-owned application managed by the CMP security consultants Krolls, used to store and communicate project designs. Access to Quickplace was provided to designated users via connection to a web site. However, the use of this system was not based on documented procedures ensuring the security of information contained within the application. In addition, the following weaknesses were noted about the configuration and administration of the Quickplace system:

(a) While system administration responsibilities had been delegated by CMP to Krolls, there were no documented procedures or terms of reference for managing and securing the information contained within the application. During the initial phases of the audit, Krolls was unable to confirm whether the application used a secure communication protocol to transmit data;

(b) There was no process in place to revoke access when users' rights and permission changed. Also, there were no rules or procedures for granting access to individual users and groups of users; and

(c) User access was not routinely monitored or validated. A list of users reviewed during the audit contained active user accounts related to staff members that were no longer employed by the UN.

49. The log files containing information about the activities performed on the Quickplace system were maintained by OICT. In consideration of the sensitivity

of the information stored in the Quickplace database used by CMP for the project designs, OIOS tested the reliability of the controls put in place for maintaining and reviewing the log files. The results of these tests highlighted the following weaknesses:

- (a) Log files were not readily available because they were maintained in an offsite location;
- (b) Periodic reviews or analyses of the log files to detect cases of misuse of unauthorized access were not performed;
- (c) The logging information pertaining to the several Quickplace databases used within the United Nations Secretariat – including the one used by CMP - were all stored in the same repository, making it difficult to isolate and monitor data specific to CMP;
- (d) The systems administrator informed OIOS that in using Quickplace they experienced poor performance as a result of limited server capability and capacity; and
- (e) OICT informed OIOS that there was no disaster recovery plan for Quickplace.

Recommendations 14 and 15

The Office of the Capital Master Plan should:

- (14) Ensure that third party contractors are aware of, and formally acknowledge the terms of reference established in ST/SGB/2004/15 for the use of ICT resources and data; and**
- (15) Assign a monitoring officer to check the security of the CMP systems, their logs, and whether users of the CMP systems comply with relevant UN policy and procedures on the use of ICT resources and data (ST/SGB/2004/15).**

50. *The Office of the Capital Master Plan accepted recommendation 14 and stated that it will send a copy of ST/SGB/2004/15 to all third party contractors. Recommendation 14 remains open pending receipt of documentation showing that third party contractors have received and acknowledged the detailed terms of reference and responsibilities for the management and security of data established in ST/SGB/2004/15 for the use of ICT resources and data.*

51. *The Office of the Capital Master Plan accepted recommendation 15 and stated that it will seek advice from OICT as to which policies and procedures should be monitored and how. Recommendation 15 remains open pending the assignment of the monitoring officer role.*

V. ACKNOWLEDGEMENT

52. We wish to express our appreciation to the Management and staff of the Office of the Capital Master Plan, OPPBA, OICT, and Skanska for the assistance and cooperation extended to the auditors during this assignment.

STATUS OF AUDIT RECOMMENDATIONS

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
1	The Office of the Capital Master Plan should establish an ICT working group/committee to review, approve, and oversee all ICT initiatives.	Governance	Medium	0	Provide copy of the formal terms of reference pertaining to the reconstituted DM ICT Committee, including evidence of oversight over CMP ICT initiatives.	Not provided
2	The Office of the Capital Master Plan should formally assign clear responsibilities to an officer, to ensure adequate administration and support of the ICT function.	Governance	Medium	0	Assign to an officer the responsibilities for the administration and support of CMP ICT issues.	Not provided
3	The Office of the Capital Master Plan should perform a risk assessment of all ICT systems supporting CMP, to identify risks and mitigating controls.	Governance	Medium	0	Document a risk assessment of all ICT systems supporting CMP.	Not provided
4	The Office of the Capital Master Plan should develop and implement an ICT model that facilitates the optimal creation, use and sharing of information between staff members.	Information Resources	Medium	0	Provide documented evidence of an ICT model developed in accordance with the UN standards established by OICT for information sharing.	Not provided
5	The Office of the Capital Master Plan should document an information module integrating both internal and external ICT applications to ensure effective systems operation, reliability and integrity of data, and continuity or recovery of operations in the event of a disaster.	Information Resources	Medium	0	Provide documented evidence of an information module integrating both internal and external ICT providers, to ensure effective systems operation, reliability and integrity of data, and continuity of operations in the event of a disaster or recovery.	Not provided
6	The Office of the Capital Master Plan should	Information	Medium	0	Provide documented evidence of	Not provided

Recom. no.	Recommendation	Risk category	Risk rating	C/O	Actions needed to close recommendation	Implementation date ²
	update internal service level agreements with OICT and OPPBA for the support of all CMP systems. These agreements should include service desk requests to process problems/errors; monitoring of requests against established internal service level agreements; and call escalation procedures.	Resources			internal service level agreements developed with OICT and OPPBA for the support of all CMP systems.	
7	The Office of the Capital Master Plan should document information security procedures, and assign responsibilities for the management and enforcement of security procedures.	Information Resources	High	O	Provide documented evidence of the CMP information security requirements.	Not provided
8	The Office of the Capital Master Plan should use the CMP website to undertake regular information security awareness sessions and to remind all stakeholders of the need to safeguard CMP information resources.	Information Resources	Medium	O	Provide documented evidence of the security awareness initiatives undertaken by CMP.	Not provided
9	The Office of the Capital Master Plan should document data access rules and requirements for all ICT systems supporting CMP and ensure they are applied to all users of the systems, including third party contractors.	Information Resources	High	O	Document data access rules and requirements for all ICT systems supporting CMP, and for all users of the systems, including third party contractors.	Not provided
10	The Office of the Capital Master Plan should document backup and disaster recovery procedures for all ICT systems supporting CMP, and develop a process for coordinating the disaster recovery plans of both internal and external users.	Information Resources	High	O	Provide documented evidence of backup and disaster recovery procedures covering all ICT systems that support CMP. Furthermore, establish that external providers have adequate backup and disaster recovery procedures to ensure the integrity of data held by them.	Not provided

Recom. no.	Recommendation	Risk category	Risk rating	C/O	Actions needed to close recommendation	Implementation date ²
11	The Office of the Capital Master Plan should conduct a business impact analysis of all ICT systems supporting CMP.	Information Resources	Medium	O	Provide documented evidence of a business impact analysis of all ICT systems supporting CMP.	Not provided
12	The Office of the Capital Master Plan should define a standard methodology to prepare, review, and approve ICT projects and initiatives, and introduce a cost-benefit analysis for ICT projects and initiatives.	Information Resources	Medium	O	Provide documented evidence of the standard project management procedures established for the ICT projects commissioned by CMP.	Not provided
13	The Office of the Capital Master Plan should document change management procedures and user acceptance test procedures to ensure that: (a) requirements are recorded and tracked even when rejected; (b) changes are recorded during the complete life-cycle of design, development and implementation phases; and (c) acceptance and approval are adequately documented.	Information Resources	Medium	O	Provide documented evidence of the change management procedures established for the ICT systems supporting CMP activities.	Not provided.
14	The Office of the Capital Master Plan should ensure that third party contractors are aware of and formally acknowledge the terms of reference established in ST/SGB/2004/15 for the use of ICT resources and data).	Governance	Medium	O	Provide documented evidence of the formal acknowledgement by third party contractors of ST/SGB/2004/15.	Not provided.
15	The Office of the Capital Master Plan should assign a monitoring officer to check the security of the CMP systems, their logs, and whether users of the CMP systems comply with relevant UN policy and procedures on the use of ICT resources and data (ST/SGB/2004/15).	Governance	Medium	O	Assign to an officer the responsibilities of monitoring the security of the ICT systems supporting CMP activities, including the verification of logs, and the compliance with UN policies and procedures.	Not provided.

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