



OIOS

Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

AUDIT REPORT

Risk mitigating measures taken for the relocation of the primary data centre of the United Nations Headquarters

Lack of planning and coordination led to significant deficiencies in the project for relocating the primary data centre

18 December 2009

Assignment No. AT2009/517/01

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 December 2009

Mr. Choi Soon-hong, Assistant Secretary-General,
Chief Information Technology Officer
Office of Information and Communications Technology

REFERENCE: IAD: 09- **03217**

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



SUBJECT: **Assignment No. AT2009/517/01 - Audit of the risk mitigating measures taken for the relocation of the primary data centre of the United Nations Headquarters**
OBJET:

1. I am pleased to present the report on the above-mentioned audit.
2. In order for us to close the remaining recommendations, we request that you provide us with the additional information as discussed in the text of the report and also summarized in Annex 1.
3. Your response indicated that OICT did not accept recommendation 7. In OIOS' opinion however, this recommendation seeks to address significant risk. We are therefore reiterating it and request reconsideration of the initial response based on the additional information provided in the report.
4. Please note that OIOS will report on the progress made to implement its recommendations, particularly those designated as high risk (i.e., recommendations 2,3 and 4), in its annual report to the General Assembly and semi-annual report to the Secretary-General.

cc: Mr. Michael Adlerstein, Assistant Secretary-General, Capital Master Plan
Mr. Warren Sach, Assistant Secretary-General, OCSS
Mr. Swatantra Goolsarran, Executive Secretary, UN Board of Auditors
Ms. Susanne Frueh, Executive Secretary, Joint Inspection Unit
Mr. Moses Bamuwanye, Chief, Oversight Support Unit, Department of Management
Mr. Byung-Kun Min, Special Assistant to USG, OIOS
Mr. Gurpur Kumar, Acting Deputy Director, Internal Audit Division, 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

ACTING DEPUTY DIRECTOR:

Gurpur Kumar: Tel: +1.212.963.5920, Fax: +1.212.963.3388,
e-mail: kumarg@un.org

EXECUTIVE SUMMARY

Audit of the risk mitigation measures taken for the relocation of the primary data centre of UNHQ

OIOS conducted an audit of the risk mitigating measures taken for the relocation of the primary data centre of the United Nations Headquarters (UNHQ). The overall objective of the audit was to assess whether adequate risk assessment and management procedures were put in place during the identification, review, and selection of the various options for the relocation of the primary data centre and the creation of a new secondary data centre. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

The General Assembly, in its resolution 63/269 dated 7 May 2009, noted “with concern the continued deficiencies in the planning and management of the project”. Since then, progress has been made to mitigate the risks inherent in relocating the primary data centre from the 19th floor of the Secretariat building, and creating a new secondary data centre.

OIOS acknowledges the difficulties experienced by the Office of Information Communication Technology (OICT) in adjusting plans due to changing circumstances and dependencies with the Capital Master Plan (CMP) project. However, OICT needed to further improve its management processes to timely address residual risks in the areas of planning, budgeting and coordination of relocation activities. For example:

- (a) Project definition, scheduling, and budget processes were inadequate;
- (b) The delay in developing the business case led to inadequate requirement specifications; and
- (c) Infrastructure assessment was weak.

Of particular note was the OICT decision to commission the new secondary data centre using existing internal resources. OICT had assumed that it could use an existing service delivery agreement with the International Computing Centre (ICC) for the provision of services to run the secondary data centre. However, the Department of Management’s (DM) decision to benchmark the ICC services resulted in ICC informing the Secretariat that it would not be able to meet the established delivery timelines. In OIOS’ view, close collaboration between OICT and DM was required to ascertain the reliability of the proposed course of action and ensure availability of resources.

TABLE OF CONTENTS

Chapter	Paragraphs
I. INTRODUCTION	1-9
II. AUDIT OBJECTIVES	10
III. AUDIT SCOPE AND METHODOLOGY	11-12
IV. AUDIT FINDINGS AND RECOMMENDATIONS	
A. Background	13-26
B. Project planning and management	27-35
C. Risk mitigation	36-41
D. Criteria, methodology and process used to select the UNFCU building	42-56
E. New arrangements proposed for the secondary data centre	57-67
V. ACKNOWLEDGEMENT	68
ANNEX 1 – Status of Audit Recommendations	

I. INTRODUCTION

1. The Office of Internal Oversight Services (OIOS) conducted an audit of the risk mitigating measures taken for the relocation of the primary data centre of the United Nations Headquarters (UNHQ). The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

2. The renovation of the Secretariat building requires the relocation of the primary data centre from the 19th floor of the Secretariat building to a temporary North Lawn facility built for the purposes of the Capital Master Plan (CMP).

3. Data centre relocation is the process of migrating data and equipment from one location to another, and presents a significant amount of risk to any organization with limited tolerance for failure. Therefore, strong risk mitigation measures are required to ensure availability of resources and skills to adequately perform the migration with minimum system downtime, and reconfiguration of any affected component, if needed.

4. As per the CMP schedule, demolition work was due to commence on the Secretariat building in November 2009 and the existing primary data centre will need to be vacated by end of March 2010. If the building is not vacated by March 2010, the CMP implementation will be subject to costly delays, with an associated cost estimated at about \$14 million per month. The risks of major disruption to the ICT infrastructure supporting the primary data centre cannot also be ruled out during the CMP construction. Therefore, it is essential to have a reliable secondary data centre to act as a backup in case of any disruption to the primary data centre.

5. To minimize system downtime during the relocation from the existing data centre, the secondary data centre needs to be fully operational by end of October 2009. The current secondary data centre in the DC2 building cannot be relied upon as a backup to run critical information technology (IT) operations during the migration. It has limited capacity for cooling and electrical power, and lacks an emergency power generator should there be a failure from the public power grid.

6. Initial plans were made, and a lease signed, for the installation of a new secondary data centre in the building of the United Nations Federal Credit Union (UNFCU) in Long Island City, New York. However, further assessments made after the signing of the lease indicated that the UNFCU building was not suitable for the installation of a new secondary data centre.

7. The General Assembly, in its resolution 63/262, Section IV paragraph 11, entitled "Information and communications technology, enterprise resource planning, and security, disaster recovery and business continuity", requested the Secretary-General to report on the risk mitigation measures to be taken during the relocation of the primary data centre to the North Lawn at the first part of its resumed sixty-third session. A proposal for a permanent solution for the

secondary data centre in the United Nations Headquarters will be submitted in the biennium 2012-2013.

8. Responsibility for the ICT infrastructure was previously that of the Information and Technology Services Division (ITSD)¹, in the Department of Management (DM). ITSD ceased to exist in January 2009 and was replaced by the new Office of Information Communications and Technology (OICT) in February 2009 with a broader mandate, and made up of resources from both ITSD/DM and ICTD/DFS.

9. Comments made by DM and OICT are shown in *italics*.

II. AUDIT OBJECTIVES

10. The main objectives of the audit were to:

(a) Assess whether adequate risk mitigation and project management procedures were put in place during the identification, review and selection of the various options for the relocation of the primary data centre and the creation of a new secondary data centre;

(b) Identify the criteria, methodology, and process used to initially select and then change the decision to use the UNFCU building in Long Island City as a suitable location for the new secondary data centre;

(c) Assess whether alternatives were considered during the determination that the UNFCU building was not a suitable location for the secondary data centre; and

(d) Determine whether the Secretary-General's report dated 26 February 2009, proposing new arrangements for the secondary data centre, was supported by an adequate business plan.

III. AUDIT SCOPE AND METHODOLOGY

11. The scope of the audit covered the activities performed by the Departments and Offices of the United Nations Secretariat involved in the decision making process for the relocation of the primary data centre. The offices included OICT; ITSD; Office of Capital Master Plan; Procurement Division; Facilities Management Division; and Office of Legal Affairs.

12. The audit methodology was based on a review of documents, including studies, analysis and budget proposals, and interviews with the officers in charge of the relevant functions. Questionnaires were also issued to relevant offices.

¹ OICT stated that OICT is not equivalent to ITSD/DM, and requested OIOS to further distinguish audit observations related to issues that arose prior to OICT's establishment in February 2009.

IV. AUDIT FINDINGS AND RECOMMENDATIONS

A. Background

13. Planning for the CMP commenced in 1999, and in June 2000 the Secretary-General submitted a report to the General Assembly (A/55/117) which explained that swing space would be required to undertake a renovation of the Headquarters building. Originally, the General Assembly adopted resolution 57/292 authorizing the Secretary-General to proceed with negotiation for the construction and lease/purchase of a swing space building (UNDC-5) by the New York State, United Nations Development Corporation (UNDC). The conceptual design for the UNDC-5 swing space included in its scope the requirement for a new primary data center that would ultimately be converted to the secondary data center following renovation of the Secretariat complex.

14. However, by September 2005, the UNDC-5 option was no longer viable (A/59/441/Add.1), as the legislature of the State of New York failed to pass the necessary legislation required to allow the use of the land for construction. The need to actively pursue acquisition of a new secondary data center became evident at the end of 2005, after it was confirmed that the UNDC-5 swing space was no longer a viable option.

15. In December 2005, the Organization decided to carry out work on the Secretariat building in four stages, in accordance with an approach entitled "Strategy IV" (also known as "Phased Strategy IV"), which would limit the amount of space to be leased in New York to relocate staff. In December 2006, the General Assembly, in its resolution 61/251, approved a project that set out new options and new deadlines, for a cost estimated at \$1.88 billion.

16. The CMP developed a plan including:

- (a) The identification of commercial off-site swing space options;
- (b) The development of a North Lawn building to meet the space needs of the Organization; and
- (c) The relocation of the primary data centre currently located in the 19th floor of the Secretariat building, to the North Lawn building.

17. In November 2006, the Board of Auditors recommended that the existing secondary data center in DC2 be relocated to a more appropriate site due to the physical proximity of DC2 to the Secretariat building.

18. In his report A/62/477, of 9 October 2007, entitled "Information and communication security, disaster recover and business continuity for the United Nations" (Part two, Section IV), the Secretary-General emphasized the urgent need to increase the size of the secondary data centre and to mitigate the potential

risk during the CMP transition. The report indicated that several site options for the secondary data centre were investigated, including the UNITAR building, 1 Met Life Plaza, the Falchi building, and the UNFCU building in Long Island City. The selection of the UNFCU building in Long Island City was justified as follows: “The benefits to be derived from the selection of Long Island City are numerous and include dual points of entry for communications; a power and communication grid different from that of the Secretariat; reduction of current lease rates to nearly half those of Manhattan; and scalability to expand as storage and service requirements grow (A/62/477, paragraph 104).”

19. However, by September 2008, following an in-depth analysis of the UNFCU Long Island City building conditions by OICT, the site was considered no longer suitable to house the secondary data centre. The analysis revealed that the costs associated with the installation of the secondary data centre would have been significantly higher than originally estimated, due to a need for structural reinforcement, fire protection and major upgrades to the electrical infrastructure.

20. The Advisory Committee on Administrative and Budgetary Questions (ACABQ), in its report A/63/487, Section IV issued on 16 October 2008, noting that the UNFCU site in Long Island City was no longer a viable option, recommended to the General Assembly not to take action on the resources requested for the UNFCU secondary data centre. ACABQ further recommended that the Secretary-General submit a new proposal for a secondary data centre, with detailed justifications on the cost already incurred on the UNFCU site.

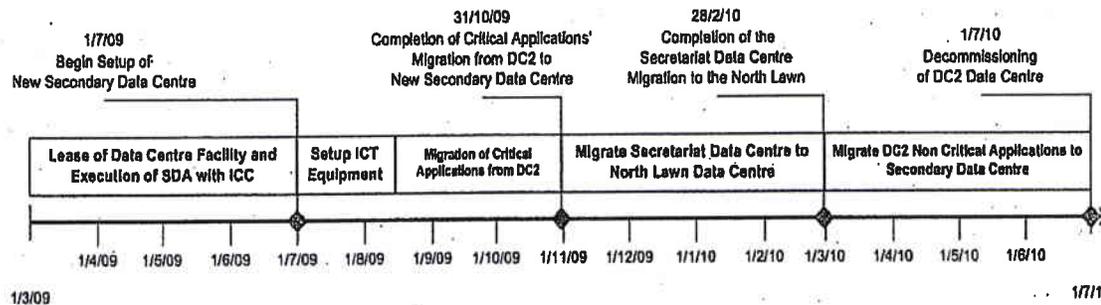
21. The General Assembly, in its resolution 63/262 of 24 December 2008, decided not to consider the proposal for a new secondary data centre at that stage, but requested the Secretary-General to report at the first part of its resumed sixty-third session on risk mitigation measures to be taken during the relocation of the primary data centre to the North Lawn.

22. Following a series of studies performed to find a new solution for the secondary data centre, another proposal was formalized by the Secretary-General in his report A/63/743, dated 27 February 2009. This proposal envisioned the following steps:

- (a) A phased relocation of the primary data centre from the Secretariat building to the North Lawn, during the period from 1 November 2009 to 28 February 2010;
- (b) Maintaining the current secondary data centre in the DC2 building in working condition throughout the entire relocation;
- (c) Leasing a commercial “infrastructure-ready” data centre facility, and installing a new secondary data centre for the period from 1 July 2009 to 31 December 2011; and
- (d) Entering into a service delivery agreement with the International Computing Centre (ICC) to manage the new secondary data centre from 1 July 2009.

23. The Secretariat developed the following timeline for the implementation of the above listed steps:

Figure 1



24. In its report A/63/774, dated 18 March 2009, the ACABQ reviewed and recommended that the General Assembly approve the new solution proposed by the Secretary-General, and fund the total estimate of \$25,737,500. However, the Committee registered serious concerns regarding the process followed by the Secretariat in mitigating the risks derived from the relocation of the primary data centre. These concerns included:

- (a) The limited amount of information contained in the Secretary-General report A/63/743, with respect to the costs that are likely to be incurred over the lifespan of the project for the new secondary data centre (A/63/774, paragraph 7);
- (b) The costs, complexity, and high risks associated with the proposed solution involving an initial temporary relocation, followed by another move to a permanent site (A/63/774, paragraph 8);
- (c) The lack of assurance from the Secretariat regarding its ability to meet the deadline for commissioning the new secondary data centre (A/63/774, paragraph 10);
- (d) The continued deficiencies in the planning and management of the project, as demonstrated by the series of events that have occurred since the Secretariat started addressing the needs arising from the relocation of the primary data centre (A/63/774, paragraph 11);
- (e) The unconvincing explanations provided by the Secretariat to justify the delays and changes made with regard to the location of the new secondary data centre (A/63/774, paragraph 12); and
- (f) The absence of a definitive classification of critical and non-critical systems, to prioritize and optimize the migration of systems in the secondary data centre.

25. The General Assembly, by its resolution 63/269 dated 7 May 2009, endorsed the recommendations made by the ACABQ. In the same document, while sharing the same concerns expressed by the Committee, the General Assembly further requested the Secretary-General to ensure full utilization of leased space, or the termination of any lease contract for space not utilized.

26. The Secretary-General in his report to the General Assembly (A/63/743) outlined plans to enter into a Service Delivery Agreement (SDA) under an existing Memorandum of Understanding (MOU) with the ICC to provide the necessary equipment and services for running the new secondary data centre. In its resolution 63/269, the General Assembly also "requested the Secretary-General, when utilizing the services of the ICC, to ensure compliance with all regulations and rules regarding procurement, in order to guarantee the cost-effectiveness of the services provided by the centre". Following the Secretary-General's proposal to use ICC, the Procurement Division (PD) initiated a benchmarking exercise by issuing a "Request for Information/Market Survey" to assess whether the ICC option represented best value for money. However, this exercise was abandoned following ICC's decision to withdraw its proposal, and stating its inability to meet the timeframe required for the installation of the new secondary data centre. Following this event, DM, in coordination with OICT, decided to undertake a comprehensive benchmarking exercise to cover a broader spectrum of ICT services, including the data centre services provided by ICC to OICT and ICTD/DFS. This new benchmarking exercise was in progress at the time of the audit. In the meantime, the ICC's withdrawal led to OICT's decision, on 18 May 2009, to proceed with the commissioning of the new secondary data centre using internal resources. OICT confirmed that this decision was taken in the absence of feasible alternatives.

B. Project planning and management

27. As indicated in the referenced reports/resolutions of the ACABQ and the General Assembly, the planning and management of the activities associated with the relocation of the primary data centre have raised serious concerns. In recent months, however, the Secretariat has made significant progress to address the concerns raised by ACABQ and the General Assembly, with the implementation of the following actions:

- (a) Recruitment of a consultancy firm specialized in data centre planning and relocation;
- (b) Identification and lease of a site in New Jersey for the new secondary data centre;
- (c) Documented "Plan B", should the "Plan A" fail;
- (d) Documented migration timeline;
- (e) Preliminary inventory of business applications; and

(f) Identification of critical applications and systems for the purposes of the relocation.

28. Although the actions listed above confirm that the Secretariat is addressing the requests of the advisory and governing bodies, OIOS reviewed the series of events related to the relocation of the primary data centre to identify control weaknesses, make recommendations to correct their causes, and prevent their recurrence in the future.

Planning, monitoring and reporting

29. Best practices in the field of data centre relocation include the creation of a project team comprised of multi-disciplinary personnel, including members from ICT operations, facilities, real estate specialists and human resources management. These teams are usually led by a dedicated project manager, who is closely aligned with the ICT organization, to drive and coordinate all activities from the planning phase through the implementation of the data migration and relocation, and after the post-move occupancy to ensure that the newly defined processes and procedures will continue to be utilized going forward. Key stakeholders should be recruited early on as advisors for the relocation project to ensure buy-in throughout the organization.

30. At the beginning of the project, ITSD did not establish a multi-disciplinary project team composed of the key functional areas and departmental stakeholders. Although OICT provided evidence of an ICT planning survey and a town-hall meeting held in 2008, the single occurrence of these events, along with the absence of a documented business plan, project management charter, detailed terms of reference, and regular meetings and status reports, confirmed the absence of proper planning and management mechanisms.

31. To address the need for a dedicated multi-disciplinary group, OICT established in June 2009 a "CMP-ICT Project Team". Since then, the team has developed detailed terms of reference comprising: i) organizational support alignment; ii) responsibility relationships; iii) timelines; iv) key project assumptions; and v) current concerns.

Recommendation 1

(1) In accordance with the principles of the recently formalized ICT project management methodology, the Office of Information and Communications Technology should establish and implement procedures for continuous monitoring and reporting on the progress of the project.

32. *OICT accepted recommendation 1 and stated that it had been monitoring the project with the assistance of a full-time project manager. In addition, senior managers have been assigned to oversee the project, constantly monitor progress and intervene to resolve issues quickly. Recommendation 1 remains open pending the receipt of documented procedures for continuous monitoring and reporting on the progress of the project.*

Inventory of systems and determination of their criticality

33. In April 2009, OICT engaged a consultancy firm specialized in data centre planning and relocation. In one of their preliminary reports issued in May 2009, the consultancy firm observed that the Secretariat “lacked a complete listing of all computer applications, because historically offices and departments either developed their own applications, hired third parties to develop applications for them, or purchased or installed application packages developed by software vendors”. In addition, OIOS noted that these applications have not been classified on the basis of their criticality.

34. OICT confirmed that as of June 2009, 89% of the applications inventory was completed. However, based on the responses provided by the Secretariat to the ACABQ in March 2009, the classification of systems is not complete, and will be addressed in response to the proposal for a unified disaster recovery and business continuity plan, as requested by the General Assembly in resolution 63/262.

Recommendation 2

(2) The Department of Management should ensure that its Business Continuity Management Unit, in collaboration with the Office of Information and Communications Technology and the other offices and departments of the Secretariat, determines the criticality of all applications and systems hosted in the United Nations data centres.

35. *The Department of Management accepted recommendation 2.* Recommendation 2 remains open pending the receipt of a document that details the criticality of the applications and systems hosted in the United Nations data centres.

C. Risk mitigation

36. The main risks associated with data centre relocations are represented by: (a) unavailability of critical systems and applications; (b) operational disruption; (c) loss of data; and (d) costly and lengthy data recovery. The cost of avoiding such threats is typically less than the cost of recovering from them.

37. It is imperative that risk mitigation measures are put in place, highlighting the critical success factors, potential obstacles and alternative solutions. Hence, it is also essential to invest the appropriate time and resources in planning, execution and testing to ensure risk mitigation. The General Assembly resolution 63/269 expressed “regret” that the proposal of the Secretary-General did not provide the necessary assurances that its implementation would sufficiently mitigate risks, including risks related to the physical security of data, during the relocation of the primary data centre to the North Lawn. OIOS also did not find evidence of a comprehensive risk mitigation process.

38. OIOS noted the following control weaknesses in the management of the project:

(a) A detailed project plan with tasks, subtasks, timelines, roles, responsibilities, dependencies, test and back-out plans were not documented early enough at the beginning of the project. The first detailed project plan was documented in April 2009.

(b) While the CMP team included a representative from the former ITSD/DM and now OICT, there were weaknesses in the allocation of responsibilities and coordination between the two main functional components, ITSD and the Office of the CMP, which ultimately led to: i) inadequate specifications and requirements for the secondary data centre facility's location and design; ii) miscalculations in budgetary requirements, space requirements, equipment densities, power, heating, ventilation & air-conditioning (HVAC) capacities, and timelines;

(c) Although OICT has documented a backup solution (plan "B") for the main plan (plan "A"), ITSD had previously not documented in a timely manner or based its plan on a detailed appraisal of all requirements. There were no procedures in place to ensure that all the risks associated with the migration of the data centre were identified and adequately addressed through an assessment and understanding of the intricacies and interdependencies that existed during data centre relocation projects.

Recommendations 3 to 5

(3) The CMP-OICT project team should develop and implement a comprehensive risk management process for the primary and secondary data centre relocation project, identifying: i) threats; ii) likelihood; iii) impact, iv) mitigating controls already in place; v) control gaps; and vi) remedial plans. The plan should be completed with information related to the office(s) responsible for implementing the remedial plans, associated costs, and the estimated timelines for completion.

The Office of Information and Communications Technology should:

(4) Ensure that the alternative measures (plan "B") are tested and operable, should the main plan ("A") fail; and

(5) Conduct a post-move assessment and review of the data centre relocation project. The evaluation should ensure completion, adequacy and security of the process. The lessons learned from the data centre move/relocation project

should be used to leverage process improvements for future projects.

39. OICT partially accepted recommendation 3 and stated that the secondary data centre relocation was nearly complete. While not formally defined with an explicit methodology, risks relating to this project have been closely monitored and proactively addressed. So, no explicit risk management plan is proposed to be undertaken at this point. This will however be undertaken for the primary data centre relocation project. Recommendation 3 remains open pending implementation of a comprehensive risk management process for the data centre relocation project.

40. OICT accepted recommendation 4 and stated that 'Plan B' consists of using the existing data centre in DC2 (as well as additional locales in the Secretariat building). 'Plan B' has been tested with critical applications. However, the limitations of this fallback option and the associated risks have been clearly documented. Recommendation 4 remains open pending receipt of documentary evidence of 'Plan B' tests undertaken.

41. OICT accepted recommendation 5 and stated that it plans to review the data centre relocation project after completion in order to leverage lessons learned for future projects. Recommendation 5 remains open pending the post-move assessment and review of the data centre relocation project.

D. Criteria, methodology and process used to select the UNFCU building

Inadequate development of a business case leading to inadequate requirement specifications, and vacant leased space

42. Best practice requires that a business case for data centre relocation includes potential costs and alternatives. Although different options were presented to the General Assembly over the course of the project, detailed feasibility studies, cost benefit and risk analysis of the various options were not undertaken at that time to determine the best solutions for the secondary data centre.

43. OIOS noted that a detailed requirement analysis or a comprehensive requirements plan was not performed before signing the lease for the UNFCU building in Long Island City. This analysis should have specified both near-term and longer-term needs for data centre operations. Included in this plan should have been details on data centre facility size, location, site plans, physical security requirements, risk management initiatives (security priorities and business continuity issues), and critical infrastructure capacities (i.e. initial estimates of equipment densities, power and cooling capacities and levels of redundancy).

44. The Secretariat entered into the lease of the UNFCU building in Long Island City without properly detailing technical specifications and requirements for the data centre. The building's inadequacy was identified late, after the

signing of the lease, following a more in-depth analysis which identified the need for additional power and adequate cooling. Rectifying this problem would have resulted in an increase in budget from \$13.2 to \$47 million, which exceeded the budget approved by the General Assembly.

45. In consideration of the actions already taken to remediate the absence of proper project management, such as the creation of a CMP-ICT project team, the hiring of a consultancy firm specialized in data centre relocation, and the recently revised ICT project management framework, OIOS is not making a recommendation on this matter. However, since the Secretariat decided not to use the UNFCU building for the installation of the secondary data centre, one floor of the building was not utilized, although the Organization was paying rent for the lease space. This matters needs to be addressed.

Recommendation 6

(6) In accordance with General Assembly resolution 63/262, the Office of the Capital Master Plan should ensure that the leased space at the UNFCU building is fully utilized, or take appropriate action to terminate the lease.

46. *The Department of Management accepted recommendation 6 and stated that the 8th, 9th and 10th floors (of the UNFCU Building) have been occupied since August 2009 and the 11th floor has been transferred to the responsibility of OCSS/FMS, and is currently being prepared for occupancy by DM/OHRM in early 2010. Recommendation 6 remains open pending confirmation of the occupancy of the UNFCU building.*

Alternative options to the construction or leasing of a secondary data centre

47. OIOS verified whether studies, reviews, and cost-benefit analysis were performed by OICT after the UNFCU building in Long Island City was deemed unsuitable, to propose new alternative solutions for the secondary data centre. OICT confirmed that an alternative option, such as cloud computing - the use of a 3rd party service to perform computing needs on a publicly accessible network - was considered unsuitable for the requirements of the United Nations Secretariat because:

(a) The diversity of the operating systems and applications environment to be supported was such that none of the market leaders in this solution could have provided the full range of platforms hosted in the existing secondary data centre;

(b) The cloud computing technology had not attained the level of maturity needed to support mission-critical applications; and

(c) There were serious concerns related to information security and control over data that would have significantly limited the type of systems for which cloud computing would have been a suitable option.

48. Additionally, OICT confirmed that “virtualization” - a technology for limiting the demand of new equipment and space in new data centre - is already used heavily in the existing data centres of the United Nations Headquarters, and will also be deployed in the new primary and secondary data centres.

49. On the basis of the information and evidence provided by OICT, OIOS did not make any recommendations in this matter, but will verify to which extent these new technologies have been used during the post-implementation audit of the new data centres.

Infrastructure assessment

50. Best practices related to data centre relocations include the documentation of a detailed inventory of the existing infrastructure, which should be analysed to determine the optimal data centre environment, the criticality of applications and systems, and the identification of obsolete equipment that do not need to be migrated. OIOS found that the Organization did not have a detailed inventory of all ICT assets with specifications regarding their physical locations, ownership, and logical access. Although ITSD initiated the inventory of the existing infrastructure in the spring of 2008, there was no evidence that this process was followed through until the recruitment of the consultancy firm specialized in data centre migration in April 2009, when they began to compile an inventory. This took place well after key decisions had been made on the data centre relocation.

51. OIOS found that there was lack of corporate ownership of ICT infrastructure within the Organization leading to:

- (a) Unclear responsibilities between the departments and OICT;
- (b) Inadequate documentation of all ICT assets; and
- (c) Lack of a standard definition for data as a result of which conditions for data access, retention requirements and security measures were not formally documented and classified in accordance with their criticality.

52. Enforcement of corporate standards for the acquisition of ICT assets was inadequate. As a result, control over the Secretariat’s information systems was ineffective, and standardized use of established technology and vendors in the ICT environment was lacking. Consequently leading:

- (a) To the migration of a large number of applications;
- (b) A high proportion of departmental applications lacked documentation or developer support; and
- (c) Backup and DR-BC test procedures for many departmental applications were lacking.

53. OICT had taken the position that departments are responsible for the migration of self-hosted applications held outside the main data centre that had been procured without OICT's knowledge. General Assembly resolution 63/262 (5 March 2009) called on the Secretariat to: (a) take a unified approach to disaster recovery and business continuity, utilizing all available infrastructure in order to achieve economies of scale and cost efficiencies, and (b) use enterprise data centres rather than local data centres as far as possible. Therefore, to prevent loss of critical UN data, regardless of their hosting arrangements (departmental self-hosted vs. OICT centrally hosted), OICT should take responsibility for migrating all applications of the UN Secretariat into an enterprise data centre.

54. According to OICT, the schedule for the data centre migrations (primary and secondary) did not provide sufficient time for moving the departmental self-hosted applications into the data centres, without increasing the risk for the migration of the applications already hosted centrally by OICT. Furthermore, OICT has provided a server room on the 6th floor of the Secretariat Building as a temporary location for these applications. OICT further stated that the implementation of General Assembly resolution 63/262 (5 March 2009) will be planned in detail and addressed as part of a separate consolidation project after the completion of the current data centre relocations.

Recommendations 7 to 8

The Office of Information and Communications Technology should:

(7) In coordination with the focal points appointed by each Department and Office, define and implement requirements to safeguard the applications hosted outside the main data centre; and

(8) Document a process for ensuring the use of enterprise data centres rather than local data centres in accordance with General Assembly resolution 63/269.

55. *OICT did not accept recommendation 7, stating that its position continues to be that departments should be responsible for the migration of self-hosted applications held outside the main data centre, as they had been procured and hosted without OICT's knowledge or approval. The tight schedule for the data centre migrations does not provide sufficient time for it to move these applications into the data centres, without increasing the risk to the migration of the applications already hosted in the data centres. OICT is assisting in mitigating the risks for these applications due to the relocation; departmental focal points for these applications have been informed and are working in close coordination with OICT to relocate the infrastructure for those applications. OICT has also commissioned and provided a temporary server room in the 6th floor of the Secretariat building, as a prelude to their eventual migration to the main data centre. The General Assembly resolution 63/262 (5 March 2009) mandate is being addressed and will be implemented as part of a separate project to consolidate data centres throughout the Secretariat. In OIOS'*

opinion, OICT needs to act as the focal point for the migration of self-hosted applications and provide departments with direction, guidelines and support for the migration of applications, and safeguard data hosted outside the main data centre. Given the criticality of data stored in departmental systems, the Organization risks the potential loss of sensitive information. Recommendation 7 remains open pending receipt of evidence documenting OICT guidelines and support to departments and offices for safeguarding and migrating applications hosted outside the main data centre.

56. *OICT accepted recommendation 8 and stated that as mandated by the General Assembly, it will be presenting a report on this matter to the 65th session, in the context of the unified disaster recovery and business continuity plan. The principles and processes for the location of applications in data centres will be promulgated in first quarter of 2011, taking note of the GA's decisions on the report to be presented. In the interim, major new enterprise systems are being hosted in either UNHQ or UNLB, depending on availability of capacity, in order to begin implementing the spirit of this mandate. Recommendation 8 remains open pending receipt of documented procedures on the use of enterprise data centres.*

E. New arrangements proposed for the secondary data centre

A temporary new secondary data centre

57. The Secretary-General in his report A/63/743 dated 27 February 2009 outlined plans to enter into a Service Delivery Agreement (SDA) with the ICC to install and manage a new temporary secondary data centre. The General Assembly in its resolution 63/269, dated 7 May 2009, entitled "Information and communications technology, disaster recovery and business continuity for the United Nations: arrangements for the secondary data centre at Headquarters", requested the Secretary-General, when utilizing the services of the ICC, to ensure compliance with all regulations and rules regarding procurement, in order to guarantee the cost-effectiveness of the services provided by the centre. In line with this request, the Procurement Division (PD) issued a Request for Information (RFI) for the provision of the services required to manage the new secondary data centre, to perform a due diligence review, and assess whether ICC's proposal represented the best-value for money option for the Secretariat. The Procurement Division received three responses to the RFI, including one from the ICC. None of the three responses, however, complied with the migration deadline established for the new secondary data centre of 1 November 2009. *OICT stated that the original proposals included both (a) the commissioning, and (b) the support, until December 2011, of the new secondary data centre. A new benchmarking exercise is already in progress for a broader range of services covering the data centres in UNHQ as well as UNLB.*

58. In view of the results of the first benchmarking exercise, OICT determined that it had no other choice than to use existing internal resources to commission the new secondary data centre, and communicated this decision in May 2009.

59. OIOS is of the opinion that the decision made by OICT to commission the new secondary data centre using its internal resources raises significant risks. The secondary data centre migration project is complex, critically interdependent with the CMP schedule, and subject to significant time constraints. It is likely that since the Secretary-General did not present in his report A/63/743 the option of using internal resources for the commissioning of the secondary data centre, this was not considered the ideal course of action.

60. OIOS acknowledges the positive steps (set-up of a dedicated project team, hiring of a specialized consulting firm, etc.) taken by OICT following its decision to commission the new secondary data centre with internal resources. However, the success of this option depends on the availability of additional resources, as requested by OICT in the following terms:

- (a) Equipment funding;
- (b) Staff augmentation;
- (c) Telecommunications links; and
- (d) Procurement support.

61. Close collaboration between the OICT and DM is therefore required to confirm the reliability of the proposed course of action, and ensure availability of all necessary resources. OICT *stated that though it agreed with the OIOS finding in paragraph 59 that the decision to commission the new data centre with internal resources raised significant risks, it had no other option left, due to the delay caused by the attempt to benchmark the ICC proposal. However, at this point of time, it does not see any practical value for this recommendation. The new temporary secondary data centre is already being commissioned using the funds approved by the General Assembly in resolution 63/269, and will be supported within the resources approved by the General Assembly. The resource requirements as well as the support structure have already been presented to the General Assembly in A/64/346/Add.1. Furthermore, a proposal for a permanent solution for the secondary data centre for UNHQ has already been requested by the General Assembly in the context of a unified ICT DR-BC plan for the Secretariat, to be presented during the 65th session.*

Engagement of the ICC

62. Relevant observations regarding the mandate and operations of the ICC have been issued by the Joint Inspection Unit (JIU) in its report JIU/REP/2000/5. The JIU noted that: "Although ICC lacks a formal statute or Inter-Agency Agreement and functions mostly like a non-binding arrangement, its role as the centre for operational IT services for the common system has steadily grown over the years..." Further commenting on the quality and efficiency of the ICC's services, the JIU also indicated that: "Comparisons with the private industry may not always be possible and even desirable for each and every common service because of some common system specificities, such as mandated operational procedures requiring the application of common system policies and rules." However, in the same document, the JIU recommended that: "Benchmarking through comparisons of like-for-like among common services within the UN

system, and/or support service units of the organizations themselves can and should be conducted regularly to identify the most efficient and cost-effective performers and methods of delivery, including outsourcing practices.”

63. With regard to entering into an agreement with ICC for the provision of the services required to manage the new secondary data centre, OIOS identified the following risks:

(a) Financial and operational risks associated with the Secretariat entering into a commitment with ICC significantly higher in value and broader in scope than the previous agreements with ICC;

(b) Risks of not having a fully functioning secondary data centre in time for the relocation of the primary data centre; and of delaying the relocation of the primary data centre from the Secretariat building at additional significant costs; and

(c) Risks of operational failure following the use of the current secondary data centre, which has limited capacity for cooling and electrical power.

64. OICT was of the view that the decision taken by DM to benchmark the ICC proposal through the issuance of a RFI was untimely and not in the best interest of the Organization. According to OICT, a direct agreement with ICC was the optimal solution, taking into account: (a) the ICC status as a main centre for operational IT services for the UN common system; (b) the pre-existing memorandum of understanding and the service delivery agreement already established in the Secretariat for the support of the primary data centre; and (c) the recent General Assembly resolution 63/262 requesting the Secretary-General to continue to utilize ICC’s services in supporting the ICT activities of the United Nations.

65. OICT further asserted that engaging ICC without the benchmarking exercise would have ensured ICC adequate time to deliver the required services in accordance with the schedule proposed in Secretary-General report A/63/743, and within equipment costs afforded by the relevant UN systems contracts. OIOS recognized that the OICT position principally rests on the need to mitigate the risks of operational failure arising from possible delays identified at the time PD communicated the decision to benchmark the ICC services.

66. OIOS also noted that DM complied with General Assembly resolution 63/269 requesting “the Secretary-General, when utilizing the services of the ICC, to ensure compliance with all regulations and rules regarding procurement, in order to guarantee the cost-effectiveness of the services provided by the Centre.” Reconciling the respective positions of DM and OICT would require both parties to fully cooperate and document the basis for entering into direct agreement with ICC.

Recommendation 9

(9) The Office of Information and Communications Technology, in close cooperation with the Department of Management, should review past and present service delivery agreements and memoranda of understanding signed by the United Nations Secretariat with the International Computing Centre (ICC), to define a standard catalogue of services to be negotiated with ICC management and identify the most cost-effective methods of delivery.

67. *OICT accepted recommendation 9 and stated that the Procurement Division has already initiated a benchmarking exercise based on a statement of work presented jointly by OICT and DFS for a range of ICT services needed from ICC. Recommendation 9 remains open pending completion of the benchmarking exercise due to be undertaken by the Procurement Division.*

V. ACKNOWLEDGEMENT

68. We wish to express our appreciation to the Management and staff of DM, OICT, and Office of Legal Affairs 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.	In accordance with the principles of the recently formalized ICT project management methodology, the Office of Information and Communications Technology should establish and implement procedures for continuous monitoring and reporting on the progress of the project.	Operational	Medium	0	Provide documented procedures for continuous monitoring and reporting on the progress of the project. Completion of the "Data Centre Migration" project.	Not provided.
2.	The Department of Management should ensure that its Business Continuity Management Unit, in collaboration with the Office of Information and Communications Technology and the other offices and departments of the Secretariat, determines the criticality of all applications and systems hosted in the United Nations data centres.	Information Resources	High	0	Provide a document that details the criticality of the applications and systems hosted in the United Nations data centres.	Not provided.
3.	The CMP-OICT project team should develop and implement a comprehensive risk management process for the primary and secondary data centre relocation project, identifying: i) threats; ii) likelihood; iii) impact, iv) mitigating controls already in place; v) control gaps; and vi) remedial plans. The plan should be completed with information related to	Governance	High	0	The implementation of a comprehensive risk management process for the data centre relocation project.	Not provided.

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
	the office(s) responsible for implementing the remedial plans, associated costs, and the estimated timelines for completion.					
4.	The Office of Information and Communications Technology should ensure that the alternative measures (plan "B") are tested and operable, should the main plan ("A") fail.	Information Resources	High	O	Provide documentary evidence of Plan B tests undertaken.	Not provided.
5.	The Office of Information and Communications Technology should conduct a post-move assessment and review of the data centre relocation project. The evaluation should ensure completion, adequacy and security of the process. The lessons learned from the data centre move/relocation project should be used to leverage process improvements for future projects.	Information Resources	Medium	O	The post-move assessment and review of the data centre relocation project.	One quarter after the completion of the project.
6.	In accordance with General Assembly resolution 63/262, the Office of the Capital Master Plan should ensure that the leased space at the UNFCU building is fully utilized, or take appropriate action to terminate the lease.	Compliance	Medium	O	Confirmation of the occupancy of the UNFCU building.	Early 2010.
7.	The Office of Information and Communications Technology should in coordination with the focal points	Information Resources	Medium	O	Provide evidence documenting OICT guidelines and support to departments and offices for safeguarding and	Not provided.

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
	appointed by each Department and Office, define and implement requirements to safeguard the applications hosted outside the main data centre.				migrating applications hosted outside the main data centre.	
8.	The Office of Information and Communications Technology should document a process for ensuring the use of enterprise data centres rather than local data centres in accordance with General Assembly resolution 63/269.	Governance	Medium	O	Provide documented procedures on the use of enterprise data centres.	Q1 of 2011.
9.	The Office of Information and Communications Technology, in close cooperation with the Department of Management, should review past and present service delivery agreements and memoranda of understanding signed by the United Nations Secretariat with the International Computing Centre (ICC), to define a standard catalogue of services to be negotiated with ICC management and identify the most cost-effective methods of delivery.	Information Resources	Medium	O	Completion of the benchmarking exercise due to be undertaken by the Procurement Division.	Not provided.

1. C = closed, O = open

2. Date provided by OICT/DM in response to recommendations.