



## INTERNAL AUDIT DIVISION

# AUDIT REPORT

---

Information and Communication  
Technology (ICT) governance in the  
Office for the Coordination of  
Humanitarian Affairs (OCHA)

OCHA needs to further strengthen its ICT  
governance model with additional controls for  
ensuring standardization of systems, security and  
efficient use of resources

14 February 2011  
Assignment No. AT2010/590/01

---

United Nations  Nations Unies

INTEROFFICE MEMORANDUM

MEMORANDUM INTERIEUR

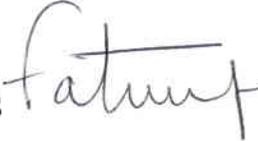
OFFICE OF INTERNAL OVERSIGHT SERVICES · BUREAU DES SERVICES DE CONTRÔLE INTERNE  
INTERNAL AUDIT DIVISION · DIVISION DE L'AUDIT INTERNE

TO: Ms. Valerie Amos, Under-Secretary-General and  
A: Emergency Relief Coordinator  
Office for the Coordination of Humanitarian Affairs

DATE: 14 February 2011

REFERENCE: IAD: 11- 00158

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



SUBJECT: **Assignment No. AT2010/590/01 - Audit of Information and Communication Technology (ICT)**  
OBJET: **Governance in the Office for the Coordination of Humanitarian Affairs**

1. I am pleased to present the report on the above-mentioned audit.
2. In order for us to close the recommendations in the OIOS recommendation database, 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 you did not accept recommendation 6. In OIOS' opinion however, this recommendation seeks to address significant risk areas. We are therefore reiterating it and requesting that you reconsider your 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 1-4, 10 and 12) in its annual report to the General Assembly and semi-annual report to the Secretary-General.

cc: Ms. Catherine Bragg, Under Secretary-General, OCHA  
Ms. Patricia Banks, Chief, Communication and Information Services Branch (CISB)  
Mr. Swatantra Goolsarran, Executive Secretary, UN Board of Auditors  
Mr. Rohan Wijeratne, Board of Auditors  
Ms. Susanne Frueh, Executive Secretary, Joint Inspection Unit  
Mr. Jonathan Childerley, Chief, Oversight Support Unit, Department of Management  
Mr. Byung-Kun Min, Special Assistant to the USG-OIOS  
Mr. Gurpur Kumar, Deputy Director, IAD, OIOS  
Ms. Amy Wong, Programme Officer, 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

**DIRECTOR:**

Fatoumata Ndiaye: Tel: +1.212.963.5648, Fax: +1.212.963.3388,  
e-mail: [ndiaye@un.org](mailto:ndiaye@un.org)

**DEPUTY DIRECTOR:**

Gurpur Kumar: Tel: +1.212.963.5920, Fax: +1.212.963.3388,  
e-mail: [kumarg@un.org](mailto:kumarg@un.org)

---

## EXECUTIVE SUMMARY

### Information and Communication Technology (ICT) Governance in the Office for the Coordination of Humanitarian Affairs (OCHA)

The Office of Internal Oversight Services (OIOS) conducted an audit of information and communication technology (ICT) governance in the Office for the Coordination of Humanitarian Affairs (OCHA). The overall objective of the audit was to assess the adequacy and effectiveness of internal controls over the OCHA ICT governance structure and operations. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

OCHA developed an ICT Operating Model (the Model) and established an ICT Governance Board (the Board) in 2009 to strengthen the governance and central control of ICT resources and adopted the Prince2 Methodology to govern ICT project management. OCHA followed the United Nations standard operating procedures on the use of ICT resources and data and for the classification of information. The ICT application architecture was adequately documented and data and system ownership was recently defined.

However, OIOS identified the following control weaknesses in ICT governance:

- (i) The objectives of the Model were not clearly aligned with OCHA's business strategy outlined in the Strategic Framework 2010-2013 and did not extend to the country/field offices. There was no formal collaboration between Information Technology Section (ITS) and Strategic Planning Unit in this regard;
- (ii) The Board did not look at strategic and policy issues. Its coverage did not extend to country/field offices, as envisaged in the Model;
- (iii) ICT was not considered a corporate function and there was no governance mechanism regarding the accountability of the Chief ITS to report to senior management and/or the Board. No reporting line or requirements existed between country/field offices and CISB;
- (iv) The structure of the ITS budget and the absence of a mechanism to recover costs limited the resources available for providing adequate oversight, guidance and standardization throughout OCHA;
- (v) Enhanced processes were needed to manage major ICT initiatives and investments, including a systematic assessment of the total cost of ownership of projects, their estimated benefits, expected quality levels and associated risks throughout their life cycle;

(vi) The ICT disaster recovery and business continuity plan did not extend to country/field offices;

(viii) There were inadequate mechanisms for access controls and there were no structured processes to formally report security incidents to Senior Management or to the Board; and

(ix) OCHA did not monitor and report on the performance of ICT service providers in accordance with the service delivery agreements or any established key performance indicators.

OIOS made a number of recommendations to mitigate the risks identified. Regarding the one case that was not accepted, OIOS provided further comments in this final report for reconsideration by OCHA Management.

## TABLE OF CONTENTS

Chapter	Paragraphs
I. INTRODUCTION	1 - 8
II. AUDIT OBJECTIVES	9
III. AUDIT SCOPE AND METHODOLOGY	10 - 11
IV. AUDIT RESULTS	
A. Planning and organizing	12 - 34
B. Acquisition and implementation	35 - 37
C. Delivery and support process	38 - 56
D. Monitoring and evaluation process	57 - 63
V. ACKNOWLEDGEMENT	64
ANNEX 1 – Status of Audit Recommendations	

---

## I. INTRODUCTION

1. The Office of Internal Oversight Services (OIOS) conducted an audit of information and communication technology (ICT) governance in the Office for the Coordination of Humanitarian Affairs (OCHA). The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

2. OCHA was established by General Assembly Resolution 46/182 of 19 December 1991 with the mandate to provide coordinated response to humanitarian emergencies. OCHA also manages Central Emergency Relief Fund (CERF) that provides interim funding for addressing humanitarian catastrophes.

3. OCHA is headquartered in New York and Geneva, with about 250 staff at each location, and operates from 27 regional, sub-regional, and country/field offices. Information and Communication Technology (ICT) operations are supported by Information Technology Section (ITS), headed by a Chief in New York and a Deputy Chief in Geneva. The NY Office primarily focuses on infrastructure and strategy, while the Geneva Office on field offices. More specifically, ITS is responsible for the development and maintenance of applications (administration, websites and databases); the provision of internal information management support (advice, guidance, standards and policies); the improvement of internal communication through OCHA's knowledge/content management systems, including the Intranet; and the coordination of inter-agency emergency ICT activities.

4. In response to the Strategic ICT assessment conducted by an ICT consulting firm in July 2008, OCHA established an IT Governance Board (the Board) in 2009. The Board's terms of reference require quarterly meeting to prioritize IT projects and approve urgent IT investment needs. The Board comprises the Chair in the Deputy of Emergency Relief Coordinator (ERC), Director New York and Geneva or their representatives, and the Chief Communication and Information Services Branch (CISB). The Chief ITS acts as Secretariat to the Board.

5. The 2010 annual budget of OCHA totalled about \$240 million and composed of 95 per cent from extra-budgetary funding and another five per cent from regular budget. Up to 13 per cent was also funded through the programme support account (PSA). An amount of \$5.3 million is allocated for ITS as detailed in Table 1.

**Table 1: ITS 2010 Financial Resource Summary**

ITS Section	Regular Budget	Extra-budgetary	Programme Support Account (PSA)	TOTAL
Geneva	0	2,997,244.00	334,800.00	<b>3,332,044</b>
New York	595,304.00	873,999.00	424,500.00	<b>1,893,803</b>
<b>TOTAL</b>	<b>595,304.00</b>	<b>3,871,243.00</b>	<b>759,300.00</b>	<b>5,225,847</b>

---

---

6. ICT solutions are being developed at OCHA field locations, to support local needs, particularly for financial management purposes. Critical IT systems include the OCHA Financial Tracking System, the CERF Admin System and OCHA Project Management System.

7. All data centre operations have been outsourced to the Department of Field Support (DFS) and are run from the United Nations Logistics Base in Brindisi, with local servers at OCHA offices for email and shared drives. The terms and conditions for the outsourcing of ICT services to DFS, United Nations International Computing Centre and Office of Information and Communication Technology (OICT) are captured in service delivery agreements. OCHA has separate websites and an intranet service (OCHANet). CERF is serviced by a web page and financial tracking databases that maintain information on Member States contributions in cash and in kind. The standards and policies issued by OICT apply to OCHA, including PRINCE2 for project management.

8. Comments made by OCHA are shown in *italics*.

## II. AUDIT OBJECTIVES

9. The overall objective of the audit was to assess the adequacy and effectiveness of the internal controls implemented in OCHA over ICT governance structure and operations, including policies and guidelines for ensuring compliance with applicable rules and regulations. Specific audit sub-objectives were to determine whether adequate control mechanisms existed for:

- (a) ICT strategic planning;
- (b) Governing ICT resources;
- (c) Managing ICT initiatives;
- (d) Establishing ICT policies, procedures and processes;
- (e) Identifying and managing ICT and related business risks; and
- (f) Ensuring business continuity and disaster recovery.

## III. AUDIT SCOPE AND METHODOLOGY

10. The audit covered the biennia 2008-09 and 2010/11. The audit methodology included the conduct of twenty interviews and/or meetings with representatives from OCHA management and key personnel in the New York and Geneva offices, and review and analysis of relevant documentation. The audit did not include site visits to field offices and Geneva.

11. The results of the risk assessment of OCHA operations that was conducted by OIOS/IAD in 2008 formed a part of the audit planning; an internal control questionnaire was also issued to further identify critical ICT systems and

---

related risks facing OCHA. Risk areas were identified for four domains: governance and strategic management; acquisition and implementation; delivery and support; and monitoring and evaluation.

## IV. AUDIT RESULTS

### A. Planning and organizing

#### Strategic management

12. Industry standards require the development of ICT strategic plans to identify ICT opportunities, capacities and limitations, goals and performance indicators, ICT resource requirements, and the desired level of investment.

13. OCHA developed an ICT operating model (the Model) in 2009 that reflected its ICT objectives and priorities. The Model included the definition of key elements in terms of focus areas and objectives, principles and resources, and in some cases, the identification of risks and benefits. However, the Model was not clearly aligned with the organization's Strategic Framework issued for 2010-2013, which was launched in June 2009. The Model did not extend to country/field offices to ensure reliable and cost-effective delivery of ICT services at Headquarters and in the field. There was insufficient evidence to show that the ICT objectives, as outlined in the Model, were well grounded in the OCHA Business Strategy to ensure that the ICT strategy supported the organization's medium- to long-term needs. There was also no evidence of formal collaboration between ITS and the Strategic Planning Unit (SPU) in this regard.

#### **Recommendation 1**

**(1) The Under-Secretary-General OCHA should ensure that the Information Technology Section, in collaboration with the Strategic Planning Unit, review the ICT Operations Model and align the objectives and strategies with the OCHA Strategic Framework for 2010-2013.**

14. *The Under-Secretary-General OCHA accepted recommendation 1 and stated that this recommendation will be implemented over the course of 2011 and incorporated in the work plans for 2012.* Recommendation 1 remains open pending receipt of a modified ICT Model and related work plans.

#### Governance

15. An ICT governance framework should ensure strategic oversight of operations, with one or more steering committees in which functional users and ICT representatives participate to prioritize ICT resources in line with organizational needs.

16. In response to the findings and recommendations of a study conducted by Gartner in July 2008, OCHA established an ICT Governance Board (the Board) in 2009, which strengthened the governance and central control of ICT

---

resources to ensure preparation, review and approval processes for ICT investments, initiatives and operations.

17. OIOS noted however, that the scope of the Board's reviews and decisions: (i) did not extend to country/field offices as envisaged in the Model and its ToR; (ii) did not include strategy and policy issues; and (iii) the minutes of its meetings were not signed.

### **Recommendation 2**

**(2) The Under-Secretary-General OCHA should modify the terms of reference and scope of the ICT Governance Board, to include responsibility for reviewing major initiatives and investments of country/field offices and approving a strategy roadmap.**

18. *The Under-Secretary-General OCHA accepted recommendation 2 and stated that OCHA recognizes the need to modify the ToRs for the IT Governance Board to look at strategic and policy issues in a more holistic and formal manner.* Recommendation 2 remains open pending receipt of a modified ToR for the Board.

### Budget resources

19. Defining capacity and resource requirements is critical for ensuring that the needs of the organization are met. OCHA did not have a formal body and/or procedure to ensure that the ICT budget was developed in line with the strategic goals of the office. In the current structure, the ICT budget is included in the budget of CISB, and each Section/Unit and country offices have their own and separate cost plans.

20. There was no chargeback and/or reimbursement policy for the technical support services provided by ITS to substantive units and country/field offices. Additionally, the cost of maintenance, including costs for administration by the ICT Governance Board, was not considered and incorporated in the project life cycle, and therefore not budgeted for

21. The ICT Governance Board proposed the establishment of a centralized pool of funds for ICT resources. However, since this proposal was not approved, OCHA has limited ability in managing the overall resource requirements for ICT operations in accordance with the strategic objectives of the office.

### **Recommendation 3**

**(3) The Under-Secretary-General OCHA should augment budgetary resources by considering an ICT cost plan that centralizes ICT resources for common products and services and by establishing mechanisms for recouping expenditure relating to services provided by ITS to programmatic sections and country/field offices.**

---

22. *The Under-Secretary-General OCHA accepted recommendation 3. Recommendation 3 remains open pending receipt of documentation showing the augmentation of OCHA's ICT budget.*

#### Organizational structure

23. An ICT organization structure should consider requirements for staff, skills, functions, accountability, authority, roles and responsibilities, which should be embedded into a framework that ensures transparency and control.

24. OCHA defined ICT roles and responsibilities in the ICT organization, but had not updated them to reflect recent restructuring. Further restructuring is envisaged in 2011 to address proposed changes in the ICT structure. ITS was housed in CISB, a programmatic office within OCHA, and was not managed as a cross-cutting function in support of the whole office. There was no reporting/governance mechanism regarding the accountability of the Chief ITS to senior management or the ICT Governance Board, and no reporting line or reporting requirements between country offices and CISB.

#### **Recommendation 4**

**(4) The Under-Secretary-General OCHA should review the organization structure and the placement of the Information Technology Section (ITS) within the Communication and Information Services Branch, ensuring that ICT forms an integral part of OCHA strategic governance framework. The review should consider relocating ITS as a separate corporate function within the organization.**

25. *The Under-Secretary-General OCHA accepted recommendation 4 and stated that OCHA may benefit from reconsidering the position of ITS within its overall structure, and was in the process of looking at a number of structural issues, which may impact reporting lines. Recommendation 4 remains open pending receipt of a report showing the results and implementation of the organizational review.*

#### Policies and procedures

26. OCHA has a formal process for updating policies and procedures and followed the standard operating procedures established by the Office of Information and Communications Technology (OICT). Specific procedures were developed to complement the organizational policies on the use of ICT resources and data (ST/SGB/2004/15) and classification of information (ST/SGB/2007/6). There were guidelines for the preparation of the budget, and procedures governing the ICT service desk, data classification, email protocol and mailing groups. The OCHA Field Connectivity Strategy V.1.1, June 2005 and Email Strategy V.1.1, July 2005 were well structured and included the required

---

technical elements. These guidelines had been promulgated on the OCHANet, but had not been updated since 2005 to ensure continued relevance.

#### **Recommendation 5**

**(5) The Under-Secretary-General OCHA should update and communicate the policies and procedures for critical information and communication technology systems and related processes.**

27. *The Under-Secretary-General OCHA accepted recommendation 5. Recommendation 5 remains open pending receipt of copies of updated ICT policies and procedures regarding critical systems and proof of dissemination OCHA-wide.*

#### Applications and systems

28. OCHA had 47 databases/systems and 40 websites with different uniform resource locators that were being developed and/or hosted by ITS on different platforms, but which had not been interfaced. There was a need to streamline the number of systems and to reassess the relevance of current systems, taking into account the total cost of ownership and ongoing United Nations Secretariat initiatives.

29. For example, the global contact system was not being used. There was also no documentation showing any assessment done regarding the replacement and/or interfacing of current systems with the United Nations' enterprise-wide initiatives being undertaken, such as the enterprise resource planning (ERP/UMOJA), customer relationship management (CRM or iNeed), and the enterprise content management system (ECM), within the context of the United Nations' ICT Strategy (A/62/793).

#### **Recommendation 6**

**(6) The Under-Secretary-General OCHA should ensure that the Information Technology Section, in collaboration with business owners, review infrastructure requirements and assess the continued relevance of current ICT systems, and prepare a roadmap for implementing, as appropriate, the United Nations Secretariat common systems/enterprise-wide applications.**

30. *The Under-Secretary-General OCHA did not accept recommendation 6 and stated that the possibilities for alignment or interfacing with enterprise applications (ERP, ECM and CRM) is a criterion for new systems or major new versions of existing systems, and that a comprehensive review of all existing systems will take resources that are not currently available in OCHA. OIOS is of the view however, that there is a need for reviewing the numerous existing applications being used in OCHA, particularly those developed before the establishment of the ICT Governance Board, in light of the new enterprise*

---

systems soon to be implemented in the United Nations Secretariat. OIOS reiterates recommendation 6, which remains open pending receipt of a report showing the results of the suggested review.

### Project management

31. OCHA maintained a portfolio of ICT projects and initiatives as part of its project management framework. The ICT Governance Board generated a matrix of approved projects and the portfolio of services was made available on the “OCHANet”. OCHA had adopted the standard project management methodology Prince2; ownership had been defined and allocated to business owners for specific applications and CISB for global applications. A review of examples of completed high level business cases (HLBCs), including the “Project Brief and Executive Summary” of the Central Emergency Relief Fund (CERF) showed that several elements of OCHA Prince2 had been applied (i.e. project management guidelines, templates, requests and project briefs and standard request format).

32. Although the format used for presenting ICT initiatives included some cost benefit and risk analysis, there was no systematic assessment of the total cost of ownership of projects, their estimated benefits, performance measurement, expected quality levels and associated risks.

### **Recommendation 7**

**(7) The Under-Secretary-General OCHA should ensure the use of Prince2 project management methodology as a standard for all projects, and implement all elements, as appropriate for the project.**

33. *The Under-Secretary-General OCHA accepted recommendation 7 and stated that the Prince 2 methodology itself does not – or rarely - recommend the use of the methodology “fully”, lest projects grind to a halt from overly heavy “process”, but to apply parts of the methodology as appropriate for the project size and type. The Under-Secretary-General also stated that risk methodology, guidelines and tolerance levels can be defined, but action mitigation plans should be decided on a case by case basis by the ICT Board, based on reports from the ICT Section.*

34. Recommendation 7 remains open pending receipt of documentation showing the application of elements such as the development of project management performance measurement criteria and the completion of total cost analyses.

## B. Acquisition and implementation

### Automated solutions and security specifications

35. New applications or functions should be reviewed to ensure that business requirements are satisfied in an effective and efficient manner. OCHA performed analyses of functional requirements and conducted feasibility studies

---

in accordance with its ICT governance framework, and presented them to the ICT Governance Board starting from 2009.

36. Application security control specifications were done on a case by case basis as required by the functional requirements analysis developed for each project. However, the security control specifications for the pre-ICT Governance Board systems had not been documented, including those for OCHA Financial Tracking System and OCHA Project Management System, critical systems that served as repository and reporting tools.

### **Recommendation 8**

**(8) The Under-Secretary-General OCHA should ensure that the Information Technology Section, in collaboration with all stakeholders, review functionality requirements and application security controls specifications of critical systems and define the desired level of security for these applications.**

37. *The Under-Secretary-General OCHA accepted recommendation 8 based on OIOS clarification of the definition of a “critical” system. OCHA further stated that as the recommendation is in respect of legacy systems (not post Gov Board application), this will be addressed in future releases of the application, in determining the trade-off between security versus cost and workability, and its own comfort level. Recommendation 8 remains open pending receipt of a report that describes functionality requirements and security control specifications of critical systems, including those existing pre-ICT Governance Board.*

## C. Delivery and support process

### ICT service management

38. Effective communication between ICT management and business customers regarding services required should be enabled by a documented definition of, and agreement on, ICT services and service levels, a process that should include monitoring and timely reporting to stakeholders on the accomplishment of service levels.

39. OIOS reviewed the Service Delivery Agreements (SDAs) established between OCHA and DFS/UNLB (Document Reference 003/08, Version 2.4, dated 01/12/2008). OCHA data centre operations were performed by the Department of Field Support (DFS) at UNLB for OCHA enterprise wide applications, such as Lotus Notes email service. OICT and the United Nations Office in Geneva (UNOG) provided support for the Supply Management Desk in Geneva. OIOS noted that OCHA did not obtain and/or review periodic reports to monitor the performance of the ICT services provided in accordance the service delivery agreements. There was no procedural requirement to collect and/or prepare the data for an annual performance report, including procedures for establishing the key performance indicators for measuring performance.

---

## Recommendation 9

**(9) The Under-Secretary-General OCHA should institute a policy and mechanism for assessing and formally reporting on the performance of all service providers, including the Department of Field Support, United Nations Logistics Base, the Office of Information and Communication Technology and third parties, in accordance with related service level agreements.**

40. *The Under-Secretary-General OCHA accepted recommendation 9.* Recommendation 9 remains open pending receipt of evidence demonstrating the development of a policy and adoption of mechanisms for performance monitoring and reporting.

### Disaster recovery and business continuity (DRBC)

41. The need for providing continuous ICT services requires developing and implementing DRBC plan, which includes maintaining and testing continuity plans to minimize ICT service interruptions and ensure timely recovery of critical business processes. OCHA had in place a disaster recovery (DR) and business continuity (BC) plan documented in the “Solution for OCHA Data Centre - New York, 11 March 2009” and the “OCHA Geneva Crisis and Continuity Management Plan, June 2009”. These plans were prepared in collaboration with current service providers (DFS, OICT and the United Nations Computing Centre, UNICC). The business continuity solutions for the data centre were well structured and included key risk elements.

42. OIOS noted that there was no documentation showing that the actions required to complete the plan were taken in accordance with the “Primary Solution and Temporary Substitute Actions” detailed in Section 6.1 of the “Business Continuity Solutions for OCHA Data Centre”. There was also no documentation of the results of any periodic tests conducted for the DRBC plan or back storage. OCHA indicated that it monitored backup results and performed periodic test-restore as needed and that more tests were anticipated following the completion of the ongoing migration of application to DFS in Brindisi.

43. OCHA had not conducted an exercise to identify all critical systems to inform the DRBC process. OCHA did not have a single framework of BC plans in accordance with the ISO standards adopted by the United Nations Secretariat (ISO/IEC 27001:2005, Ref: A.14.1.4). The ICT DRBC plan did not extend to business processes to ensure continuity of country/field operations. This condition exposes OCHA to the risk of ineffective alignment of field offices’ operations with the continuity plans defined for OCHA Headquarters in New York and Geneva.

---

## Recommendations 10 and 11

**(10) The Under-Secretary-General OCHA should, in coordination with the Department of Field Support, United Nations Logistics Base and the Office of Information and Communication Technology, document the criteria for identifying critical applications within the general business continuity framework of OCHA, and define procedures for country/field offices.**

**(11) The Under-Secretary-General OCHA should establish a single framework of business continuity plans in accordance with the international standard adopted by the United Nations Secretariat (ISO/IEC 27001:2005 Ref: A.14.1.4) and ensure that all plans are consistent regarding security requirements, and contain priorities for testing, analyzing results and maintenance.**

44. *The Under-Secretary-General OCHA accepted recommendation 10 and stated that identifying critical systems can be done, but OCHA doubts whether having only one level of distinction (critical/non-critical) is useful; there should be multiple levels. Regarding country/field offices, SPU will work with ITS to ensure coherence and integration of OCHA NY's business continuity plan with ITS's disaster recovery plan. Recommendation 10 remains open pending receipt of documentation demonstrating the adoption of criteria for the identification of critical systems.*

45. *The Under-Secretary-General OCHA accepted recommendation 11. Recommendation 11 remains open pending receipt of documentation showing that a single business continuity framework has been developed in accordance with ISO standards and consistently applied OHCA-wide.*

### Investigation into OCHA Geneva data losses

46. The status of implementation of the recommendations made in the report of the "The investigation into OCHA Geneva Data Losses in November 2008" carried out by an independent consultant, Linksbridge, had not been documented. Several recommendations were made with regard to: (i) DRBC and the use of shared drive versus ad-hoc data storage; (ii) strengthening the ICT infrastructure; (iii) ICT performance issues; (iv) ownership of ICT solutions; (v) accountability for the 2008 data loss and breach of United Nations standards; and (v) investing in ICT sourcing and supplier management capabilities.

## Recommendation 12

**(12) The Under-Secretary-General OCHA should address all recommendations made in the "Investigation into OCHA Data Losses in November 2008", and update the current business continuity and disaster recovery plan accordingly.**

---

47. *The Under-Secretary-General OCHA accepted recommendation 12. Recommendation 12 remains open pending receipt of a status report showing that all recommendations documented in the report “The investigation into OCHA Geneva Data Losses in November 2008” have been addressed.*

### Security

48. Maintaining the integrity of information and protect ICT assets requires a security management process that includes establishing roles and responsibilities, policies, standards, and procedures, in accordance with best practices such as ISO-27001 as adopted by the United Nations Secretariat. OCHA followed the policies and procedures established by the United Nations Secretariat regarding information security management, including specific guidelines for reporting stolen equipment/mobile devices as part of documented security incident policy, but had not done any ICT-specific training requirements on security awareness.

49. In addition, ICT security threat and vulnerability assessments and periodic reporting covering intrusion, data loss and non-performance were not done. OCHA did not have a policy and mechanisms in place for performing regular reviews of user access to critical applications, for enforcing the selection of strong passwords and require regular changes/updates by all users, and for encrypting the hard drives of the laptops used as mobile offices. There were no particular ICT control mechanism in place for critical systems such as the Financial Tracking System and OCHA Project Management System that process and store sensitive information.

### **Recommendations 13 to 14**

#### **The Under-Secretary-General OCHA should ensure that the Information Technology Section:**

**(13) Assess system risks, and periodically report to the IT Governance Board on potential security risks, including the analysis and actions taken following the conduct of any vulnerability test;**

**(14) Establish security policy measures for laptops and perform regular review of user access to, and the selection of strong passwords on, all critical servers, operating systems and applications.**

50. *The Under-Secretary-General OCHA accepted recommendation 13 and stated that ITS will report system risks to the new ICT committee. Recommendation 13 remains open pending receipt of copies of the security risk reports provided to the ICT Committee or IT Governance Board.*

51. *The Under-Secretary-General OCHA accepted recommendation 14. Recommendation 14 remains open pending receipt of a set of policies and*

---

procedures on ICT security for ensuring, inter alia, regular review of user access; selection and changing of passwords; and security of mobile systems.

Configuration, change and incident management

52. Service, change and incident management procedures should allow a timely and effective response to ICT user queries and problems, by registering and escalating problems/incidents, and performing trend and root cause analysis and resolutions. OCHA established service desks in the New York and Geneva offices that included partial coverage of field offices, and incident ticketing and error logs were captured as part of the Service Desk Ticket system. While incidents/problems were analyzed, a structured reporting process had not been implemented, no user satisfaction reports were generated and an ICT incident management process was not documented.

53. OIOS noted that there was no mechanism to formally report to senior management on security incidents, although security incidents like the web-hacking of the humanitarian information home page that occurred in February 2010, and instances of unauthorized access, were reported and remedial actions taken. Incident reports did not include adequate information related to the steps taken to resolve the issues and prevent their recurrence. The “next steps” section of the reports did not include adequate information and details documenting “who, when and how steps have been taken”. For example, there was no documentation of the results of the “next steps” on the “2010.02.20 Hacking of humanitarianinfo homepage” relating to the investigation of ITS logs.

54. OCHA did not maintain ICT configuration details for critical systems and applications (where and how to apply the fix), but planned to do so as part of the ongoing initiative to use the iNeed application/customer relationship management (CRM).

**Recommendations 15 and 16**

**The Under-Secretary-General OCHA should:**

**(15) Formalize an ICT change and incident management procedure and assign accountability for documenting it, including logging, tracking, resolutions, reporting and monitoring; and**

**(16) Ensure that the Information Technology Section conduct periodic internal client satisfaction survey (including country/field offices) to obtain feedback regarding the adequacy of ICT support services provided by ITS.**

55. *The Under-Secretary-General OCHA accepted recommendation 15. Recommendation 15 remains open pending receipt of a copy of the incident management procedure that clearly addresses identified gaps.*

---

56. *The Under-Secretary-General OCHA accepted recommendation 16.* Recommendation 16 remains open pending receipt of a copy of the analysis of ICT survey results.

#### D. Monitoring and evaluation process

##### Monitor and evaluate ICT performance and controls

57. Effective management of ICT systems and services should be accomplished by clearly defining the roles, responsibilities and expectations in service level agreements - either internal, between ICT and functional offices or external with third party providers - to minimize the risks associated with non-performance, poor quality services and disruption of work. ITS-Geneva managed OCHA application architecture and maintenance of field ICT activities, while ITS-New York managed ICT (infrastructure) architecture, strategic services and service desk.

58. OIOS noted that OCHA made progress in the following ICT areas: (i) enhancement of the information management and technology with the establishment of the ICT Governance Board and portfolio management; (ii) outsourcing and consolidation of the data centre in UNLB/Brindisi; (iii) coding of applications to “Trygin” in India; (iv) establishment of a service desk role; and (v) development of a DRBC plan and back-up policy.

59. However, there were no formal requirements and procedures for a comprehensive monitoring, evaluation of and reporting on ICT performance both at Headquarters and in the country/field offices, although performance reports and statistics were available for websites and other web hosted applications. OIOS noted that OCHA did not generate periodic reports on historical risk trends and events, and did not prepare remedial action plans. Also, while a service catalogue was in place for field offices, there was no catalogue of the services provided at OCHA Headquarters in support of programmatic areas to serve as a checklist for ascertaining value and quality of services delivered, and no user satisfaction reports.

#### **Recommendation 17**

**(17) The Under-Secretary-General OCHA should ensure that the Information Technology Section establish operating level agreements with relevant business owners within OCHA, including country/field offices, and formalize standard monitoring and performance reporting procedures to the senior management team and ICT Governance Board.**

60. *The Under-Secretary-General OCHA accepted recommendation 17.* Recommendation 17 remains open pending receipt of copies of established operating level agreements, a standard monitoring and reporting format and a checklist of services provided.

---

## Results of external reviews

61. OCHA had not conducted any self-assessment and reported on the effectiveness of ICT controls. OCHA commissioned two external reviews: (i) the information management review in 2007; and (ii) the strategic ICT assessment in 2008. The results of the reviews were detailed in reports and recommendations aimed at improving the ICT function. However, OIOS noted that OCHA had not established a process to systematically review, monitor and report on the implementation status of these recommendations. As of the time of the audit, the status of implementation of the recommendations issued as a result of the external reviews was as follows:

- (i) Information management review (2007): The recommendation to create an organization-wide, cross-cluster knowledgebase for key humanitarian information and analysis was partially implemented; the data audit, and the design and scope for the centralized global database were outstanding; and
- (ii) ICT strategic assessment (2008): The following issues were outstanding: change in organizational structure; budgeting system; application development and architectural standards, methodology, testing and documentation.

### **Recommendations 18 and 19**

**The Under-Secretary-General OCHA should:**

- (18) Conduct self-assessments of and report on ICT controls based on established key performance indicators;**
- (19) Review the implementation status and develop an action plan to fully address the ICT related recommendations from external reviews.**

62. *The Under-Secretary-General OCHA accepted recommendation 18. Recommendation 18 remains open pending receipt of the results and analysis of any ICT self-assessments.*

63. *The Under-Secretary-General OCHA accepted recommendation 19 and stated that as with all reviews and evaluations, Senior Management agrees on the critical recommendations that require implementation. ICT will ensure implementation of only those recommendations which are approved by the Senior Management Team. The USG also stated that SPU recently created an audit/evaluation tracking database, in cooperation with CISB, which will be used to help management follow up and report on recommendations made in audits, evaluations and reviews. Recommendation 19 remains open pending receipt of a status report showing the actions taken to address all recommendations, and indicating how the related risks are being mitigated for those not accepted.*

---

## V. ACKNOWLEDGEMENT

64. We wish to express our appreciation to the Management and staff of OCHA 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 <sup>1</sup>	Actions needed to close recommendation	Implementation date <sup>2</sup>
1	The Under-Secretary-General OCHA should ensure that the Information Section, in collaboration with Strategic Planning Unit, review the ICT Operations Model and align the objectives and strategies with the OCHA Strategic Framework for 2012-2013.	Governance	High	O	Receipt of a modified ICT Model that is aligned with the Strategic Framework, and related activities reflected in the work plans.	31/12/2011
2	The Under-Secretary-General OCHA should modify the terms of reference and scope of the ICT Governance Board, to include responsibility for reviewing major initiatives and investments for country/field offices, and approving a strategy roadmap.	Governance	High	O	Receipt of the modified ToR, including the recommended changes.	31/12/2011
3	The Under-Secretary-General OCHA should augment budgetary resources by considering an ICT cost plan that centralises ICT resources for common products and services and establishing mechanisms for recouping expenditure relating to services provided by ITS to programmatic sections and country/field offices.	Governance	High	O	Receipt of documentation showing the augmentation of OCHA's ICT budget.	31/12/2012
4	The Under-Secretary-General OCHA should review the organization structure and the placement of the Information Technology Section (ITS) within the Communication and Information Services Branch, ensuring that ICT forms an integral part of OCHA strategic governance framework. The review should consider relocating ITS as a separate corporate function within the organization.	Governance	High	O	Receipt of a report showing the results and implementation of the organizational review.	31/12/2012
5	The Under-Secretary-General OCHA should update and communicate policies and procedures for critical information and communications technology systems and related processes.	Governance	Medium	O	Receipt of copies of updated ICT policies and procedures.	31/12/2011

Recom. no.	Recommendation	Risk category	Risk rating	C/O <sup>1</sup>	Actions needed to close recommendation	Implementation date <sup>2</sup>
6	The Under-Secretary-General OCHA should ensure that the Information Technology Section, in collaboration with business owners, review infrastructure requirements and assess the continued relevance of current ICT systems and prepare a roadmap for implementing, as appropriate, the United Nations Secretariat common systems/enterprise-wide applications.	Governance	Medium	O	Receipt of a report showing the results of the recommended review of OCHA's applications.	Not provided
7	The Under-Secretary-General OCHA should ensure the use of Prince2 project management methodology as a standard for all projects, and implement all elements, as appropriate for the project.	Governance	Medium	O	Receipt of documentation showing the application of elements such as the development of project management performance measurement criteria and the performance of total cost analysis for projects.	31/07/2012
8	The Under-Secretary-General OCHA should ensure that the Information Technology Section, in collaboration with all stakeholders review functionality requirements and application security controls specifications of critical systems and define the desired level of security for applications.	Operational	Medium	O	Receipt of a report that describes functionality requirements and security controls specifications of all critical systems, pre-ICT Governance Board.	Not provided
9	The Under-Secretary-General OCHA should institute a policy and mechanism for assessing and formally reporting on the performance of all service providers, including the Department of Field Support, United Nations Logistics Base, the Office of Information and Communication Technology and third parties, in accordance with related service level agreements.	Operational	Medium	O	Receipt of a mechanism and related policy on performance management and reporting.	31/12/2011
10	The Under-Secretary-General OCHA should, in coordination with the Department of Field Support, United Nations Logistics Base and the Office of Information and Communication Technology, document the criteria for identifying critical applications within the general business continuity framework of OCHA, and define procedures for country/field	Operational	High	O	Receipt of documentation demonstrating the establishment and adoption of criteria for identification of critical systems, and documentation in a section in the BCP that describes the expectations of ITS regarding the field.	31/7/2012

Recom. no.	Recommendation	Risk category	Risk rating	C/O <sup>1</sup>	Actions needed to close recommendation	Implementation date <sup>2</sup>
	offices.					
11	The Under-Secretary-General OCHA should establish a single framework of business continuity plans in accordance with the international standard adopted by the United Nations Secretariat (ISO/IEC 27001:2005 Ref: A.14.1.4) and ensure that all plans are consistent regarding security requirements, and contain priorities for testing, analyzing results and maintenance.	Operational	Medium	O	Receipt of documentation showing that a single BCP framework has been established and consistently applied OCHA-wide.	31/12/2011
12	The Under-Secretary-General OCHA should address all recommendations made in the “Investigation into OCHA Data Losses in November 2008”, and update the current business continuity and disaster recovery plan accordingly.	Operational	High	O	Receipt of a status report showing that all control weaknesses have been addressed.	31/12/2011
13	The Under-Secretary-General OCHA should ensure that the Information Technology Section assess system risks, and periodically report to the IT Governance Board on potential security risks, including the analysis and actions taken following the conduct of any vulnerability test;	Operational	Medium	O	Receipt of copies of risk report provided to ICT Committee or IT Governance Board.	31/12/2011
14	The Under-Secretary-General OCHA should ensure that the Information Technology Section establish security measures for laptops and perform regular reviews of user access to, and the selection of strong passwords on, all critical servers, operating systems and applications.	Operational	Medium	O	Receipt of a set of policies and procedures on ICT security for ensuring, inter alia, the following: regular review of user access, selection and changing of passwords and security of mobile systems, as deemed appropriate.	31/12/2011
15	The Under-Secretary-General OCHA should ensure that the Information Technology Section formalize the ICT incident management procedure and assign accountability for documenting it, including logging, tracking, resolutions, reporting and monitoring;	Operational	Medium	O	Receipt of a copy of the incident management procedure that clearly addresses identified gaps.	31/12/2011
16	The Under-Secretary-General OCHA should ensure that the Information Technology Section to conduct periodic internal client satisfaction	Operational	Medium	O	Receipt of a copy of the analysis of ICT survey results.	30/06/2011

Recom. no.	Recommendation	Risk category	Risk rating	C/O <sup>1</sup>	Actions needed to close recommendation	Implementation date <sup>2</sup>
	survey (including country/field offices) to obtain feedback regarding the adequacy of ICT support services provided by ITS.					
17	The Under-Secretary-General OCHA should ensure that the Information Technology Section establish operating level agreements with relevant business owners within OCHA, including country/field offices, and formalize standard monitoring and performance reporting procedures to the senior management team and ICT Governance Board.	Operational	Medium	O	Receipt of copies of established operating level agreements, a standard monitoring and reporting format and a checklist of services provided.	31/12/2012
18	The Under-Secretary-General OCHA should ensure that the Information Technology Section conduct self-assessments of and report on ICT controls based on established key performance indicators.	Operational	Medium	O	Receipt of the results and analysis of any ICT self-assessments, and the criteria/key performance indicators established as the basis.	31/12/2011
19	Review the implementation status and develop an action plan to fully address the ICT related recommendations emanating from external reviews.	Operational	Medium	O	Receipt of a status report showing action taken for all recommendations what are accepted by OCHA management, and explanation for those not accepted and implemented.	Not provided

1. C = closed, O = open

2. Date provided by OCHA in response to recommendations.