



OIOS

Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

AUDIT REPORT

Information and Communication Technology Governance and Security Management at the United Nations Framework Convention on Climate Change

**Although fundamental controls and procedures
are in place, some weaknesses, if not addressed,
could expose UNFCCC to significant risks**

4 November 2009

Assignment No. AT2008/241/01

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: Mr. Yvo de Boer, Executive Secretary
A: United Nations Framework Convention on Climate
Change

DATE: 4 November 2009

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

REFERENCE: IAD: 09- 03082

SUBJECT: **Assignment No. AT2008/241/01 - Audit of Information and Communication Technology
Governance and Security Management at the United Nations Framework Convention on
Climate Change**

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. Please note that OIOS will report on the progress made to implement its recommendations, particularly those designated as high risk (i.e., recommendations 1,2,13 and 19) in its annual report to the General Assembly and semi-annual report to the Secretary-General.

cc: Mr. Richard Kinley, Deputy Executive Secretary, UNFCCC
Mr. Kevin Grose, Coordinator, Information Services Programme, UNFCCC
Mr. Swatantra Goolsarran, Executive Secretary, UN Board of Auditors
Ms. Suzanne Frueh, Executive Secretary, Joint Inspection Unit
Mr. Moses Bamuwamye, Chief, Oversight Support Unit, Department of Management
Mr. Byung-Kun Min, Special Assistant to the USG, OIOS
Mr. Normand Ouellet, Chief, Nairobi Audit Service, OIOS

INTERNAL AUDIT DIVISION

FUNCTION

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

CONTACT INFORMATION

ACTING DIRECTOR:

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

CHIEF, NAIROBI AUDIT SERVICE:

Normand Ouellet: Tel: +254.20.762.5391, Fax: +254.20.624.125,
e-mail: normand.ouellet@unon.org

EXECUTIVE SUMMARY

Audit of information and communications technology governance and security management

OIOS conducted an audit of information and communications technology (ICT) governance and security management at the United Nations Framework Convention on Climate (UNFCCC). The overall objective of the audit was to determine whether UNFCCC has adequate controls in place to govern and protect ICT resources. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

OIOS found that in general, the ICT operations at UNFCCC were well organized. Fundamental controls and procedures for ICT planning, support, and security were in place, such as ICT budget plans; catalogue of ICT services; guidelines for the use of email and network resources; business impact analysis and risk assessment; hardware and software policies; standards for records and content management; and service level agreements.

However, the results of the audit highlighted some control weaknesses that if not addressed by management, could expose UNFCCC to the risks of inefficient and ineffective use of resources, and breaches in the security of systems and data. In particular, OIOS identified that:

- (a) New criteria and mechanisms are needed to develop the ICT strategy and monitor its implementation;
- (b) ICT performance indicators do not adequately measure the activities monitored;
- (c) An information architecture and process framework is not available;
- (d) ICT operations are not assessed nor monitored on the basis of pre-defined criteria and metrics;
- (e) Service desk requests and operation level agreements are not managed on the basis of standard procedures and metrics;
- (f) ICT training needs are not consistently assessed and plans implemented;
- (g) Change requests and user acceptance tests are not supported by documented procedures and tools;
- (h) There are no information security policies and procedures; and
- (i) The business continuity system is based on draft terms of reference and procedures.

TABLE OF CONTENTS

Chapter	Paragraphs
I. INTRODUCTION	1-7
II. AUDIT OBJECTIVES	8
III. AUDIT SCOPE AND METHODOLOGY	9-12
IV. AUDIT FINDINGS AND RECOMMENDATIONS	
A. ICT strategic planning and governance	13-23
B. Information architecture	24-29
C. ICT investments	30-32
D. ICT operations	33-46
E. ICT security	47-61
V. ACKNOWLEDGEMENT	62
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 and security management at the United Nations Framework Convention on Climate Change (UNFCCC). The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.
 2. UNFCCC and the Kyoto Protocol are serviced by the Secretariat, also known as the "Climate Change Secretariat" (Secretariat), whose mandate is laid out in general terms in Article 8 of the Convention.
 3. The main functions of the Secretariat are to:
 - (a) Make practical arrangements for sessions of the Convention and Protocol bodies;
 - (b) Monitor implementation of the commitments under the Convention and the Protocol through collection, analysis and review of information and data provided by the Parties;
 - (c) Assist the Parties in implementing their commitments;
 - (d) Support negotiations, including through the provision of substantive analysis;
 - (e) Maintain registries for the issuance of emission credits and for the assigned amounts of emissions of the Parties that are traded under emission trading schemes;
 - (f) Provide support to the compliance regime of the Kyoto Protocol; and
 - (g) Coordinate with the secretariats of other relevant international bodies, notably the Global Environment Facility (GEF) and its implementing agencies United Nations Development Program (UNDP), United Nations Environmental Program (UNEP), and the World Bank (WB), the Intergovernmental Panel on Climate Change (IPCC), and other relevant conventions.
 4. Specific tasks included the preparation of official documents for the Conferences of the Parties (COP) and subsidiary bodies; coordination of In-Depth Reviews of Annex I Party national communications; and the compilation of greenhouse gas inventory data.
 5. The Information Services (IS) programme supports the mandated work of all other programmes of UNFCCC by maintaining availability of the public website and Intranet, informing the general public of climate change objectives and activities, and promoting media relations.
 6. The budget performance for the biennium 2006- 2007 presented detailed data regarding the activities conducted by the Information Services in three main
-

domains: (a) ICT; (b) knowledge management; and c) communications and media relations. The main results achieved during the biennium, included:

- (a) A globally accessible website (unfccc.int), used as the main external portal for UNFCCC data, documents and information;
- (b) Enhancement of the UNFCCC website through the provision of targeted information for the Parties, observers and the general public, including online newsletters, articles and news announcements published on the home page;
- (c) Provision of webcast services;
- (d) Production of 10 publications and 24 presentations on the climate change process and the work of the UNFCCC secretariat to the general public;
- (e) Implementation of a records management programme and policy framework for the Secretariat;
- (f) Management of a secure information and communication technology infrastructure, with 500 network end points for a user community of about 300 staff, consultants, contractors and interns;
- (g) Extension of the network to accommodate the entire Secretariat after the consolidation of all staff at the "Haus Carstanjen" location in Bonn;
- (h) Support for laptop users;
- (i) Deployment of a consolidated electronic data storage solution providing about 2,000 gigabytes of storage capacity for headquarters operations;
- (j) Deployment of a mobile storage solution of about 1,600 gigabytes capacity providing support to UNFCCC conferences;
- (k) Implementation of the new secretariat-wide information infrastructure; and
- (l) Completion of the second phase of implementation of the business continuity planning for the whole secretariat, that included a full analysis of secretariat systems, the risks associated with those systems and an agreed framework on the maximum tolerable outages for each.

7. Comments made by UNFCCC are shown in *italics*.

II. AUDIT OBJECTIVES

8. The main objectives of the audit were to assess the adequacy and effectiveness of internal controls to ensure that:

- (a) ICT governance strategic planning and processes exist;
- (b) Roles and responsibilities for ICT governance, operations and security are defined;
- (c) Terms of reference exist and are followed for ICT initiatives, projects and operations;
- (d) Procedures are in place for ICT risk assessment and management of critical operations, applications and systems;
- (e) ICT operations and use of ICT resources and data are monitored;
- (f) Sensitive data and information are protected; and
- (g) Appropriate disaster recovery and business continuity plans exist.

III. AUDIT SCOPE AND METHODOLOGY

9. The audit included a review of the policies, standard operating procedures, and guidelines in place at the UNFCCC Secretariat in Bonn concerning ICT governance and security management.

10. The audit team used internal control questionnaires, interviewed representatives from the Administration Services, Information Services, substantive programmes, and the records management office.

11. Site visits were conducted to review the physical installations at Haus Carstanjen and Langer Eugen.

12. Network vulnerability tests were conducted on selected critical hosts.

IV. AUDIT FINDINGS AND RECOMMENDATIONS

A. ICT strategic planning and governance

UNFCCC needs a mechanism to develop and oversee its ICT strategy

13. ICT services at UNFCCC are currently delivered by the Information Services programme which is also mandated to deliver services in the areas of knowledge management and communications, and media relations. The Information Service programme provides ICT infrastructure (networks, telecommunication systems, hardware and user support), and hosting services both at the UNFCCC's Secretariat headquarters in Bonn, as well as for conferences at their different locations.

14. In addition to Information Services, two substantive programmes have a significant Information Services component, supported by their own teams. These include the "Reporting, Data and Analysis" (RDA), and the "Sustainable Development Mechanisms" (SDM) programmes. While according to UNFCCC there is no authoritative way to measure the overall ICT budget, they estimated it at \$12 million annually.

15. UNFCCC does not have a high level committee on ICT that would ensure that: (a) ICT is adequately considered in the overall governance process of the Organization; (b) ICT strategic direction is defined; and (c) major ICT initiatives and investments are reviewed.

16. UNFCCC also does not have an ICT Strategy. An ICT strategy should define how the ICT function supports the Organization in achieving its strategic objectives, identifying responsibilities, accountabilities, resources, risks, and costs.

17. Responding to a request of its Executive Secretary to develop a vision for its information systems, UNFCCC launched in September 2008 a due diligence review to define the ICT governance model for the Organization. The review yielded a "roadmap" document, which outlined a plan to establish an Organization-wide ICT governance framework under several different scenarios. The "roadmap" documented a thorough analysis of risks, costs, timelines, scenarios and options. Selecting the preferred scenario was left to the decision of senior UNFCCC management, before forwarding a recommendation to the Management Team.

18. In the absence of an organization-wide ICT strategy, and a high level committee on ICT, UNFCCC has been unable to adequately identify and address the potential risks deriving from the use of ICT resources, and to exploit the opportunities presented by new ICT capabilities.

Recommendations 1 and 2

(1) UNFCCC should formalize its ICT governance model by completing the September 2008 due diligence review.

(2) Following the formalization of an ICT governance model, UNFCCC should establish an ICT Strategic Committee, with a mandate to ensure that:

(a) all programmes and services are adequately represented;

(b) the decision-making process is based on clear terms of reference;

(c) performance evaluation processes and criteria are defined; and

(d) an ICT strategy is developed.

19. *The UNFCCC Administration accepted recommendation 1 and stated that it completed the roadmap to IT governance in November 2008, and the IT governance implementation plan was scheduled to be completed in August 2009 and to be submitted to the Management Team for approval. Recommendation 1 remains open pending receipt of documentation of a formalized ICT Governance Module.*

20. *The UNFCCC Administration accepted recommendation 2 and stated that subject to the Management Team's approval of the IT governance implementation plan, the managerial arm of governance, the Information Technology Management Committee is scheduled to be operational in March 2010 and the ICT strategy is scheduled to be developed by the technical panel in 2010. Recommendation 2 remains open pending implementation of the IT management committee and documentation of an ICT strategy.*

ICT performance indicators

21. The planning document in support of the 2010-2011 biennium budget for the sub-programme related to information services and communication technology has been articulated on four objectives. The plan detailed information about objectives, sub-objectives, performance indicators, requirements, costs, and funding resources. OIOS noticed that the plan was developed on the basis of the professional industry standard "Control objectives for information and related technology" (Cobit).

22. With the definition of a detailed planning document that included performance indicators, UNFCCC has taken a positive step towards the creation of an internal control system for monitoring and managing the ICT function. However, as a result of the review conducted, the plan presents some limitations, such as:

(a) Performance indicators not aligned with the objectives. This problem was identified in several instances. For example, in the case of

“server infrastructure” the stated objective was defined as follows: “to maintain the existing virtual and physical server infrastructure at its current level to continue operating existing secretariat-wide and mandated information system”. The corresponding performance indicators were: “all hardware and software in productive use properly licensed and covered by respective support contracts”, and “sufficient staff available to cover agreed operational levels”. While the elements identified in the performance indicators are necessary components to achieve the objective, they do not adequately express a measurement of performance;

(b) The plan does not indicate which source of data provides the indicators adopted for the monitoring process of each objective; and

(c) The plan does not include adequate information for monitoring and comparing the performance achieved during an adequate timeframe (i.e. three years). These analyses and comparisons would allow UNFCCC to identify trends, compare performance, and better support the decision making process.

Recommendation 3

(3) UNFCCC should review its ICT planning document to ensure that performance indicators adequately express a measurement of the activities monitored.

23. *The UNFCCC Administration accepted recommendation 3 and stated that the 2010/1011 biennium plan prepared by Information Communication Technology Operations will re-align objectives (using the SMART concept) and indicate the sources of data with time-bound monitoring processes. UNFCCC further stated that it will also apply this to planning documents prepared for Information Service Delivery once it starts its function in accordance with the organizational IT governance structure. Recommendation 3 remains open pending receipt of planning documentation that includes performance indicators as a measurement of activities monitored.*

B. Information architecture

Need for an information architecture and process framework

24. UNFCCC developed a “Concept Paper” on a Secretariat-wide “Information Architecture Plan” (Plan). The purpose of the Plan was to provide a set of organizational standards for validating information systems’ implementation, and their alignment with the organizational goals of UNFCCC.

25. In 2006, the Board of Auditors recommended inter-alia that UNFCCC should develop an information architecture plan. UNFCCC accepted the recommendation but has yet to implement it beyond the “Concept Paper” mentioned above.

26. However, in the absence of defined process controls in support of the information architecture plan, UNFCCC would not be able to achieve a consistent approach to information systems management, avoid duplications, and maximize the use of applications.

27. In the current situation, UNFCCC is exposed to the risks of inconsistencies between the various programmes in collecting, processing, storing, and reporting data. This condition could also cause the accumulation of data that is not relevant, consistent or usable in an economical manner.

Recommendations 4 and 5

UNFCCC should:

(4) Develop standard process controls for managing information systems, requiring the definition of: (a) Key roles and responsibilities; (b) Process ownership; (c) Templates for data collection and reporting; and (d) Criteria and procedures for quality assurance and continuous improvement.

(5) Complete the development of its information architecture plan and create a centralized repository of all applications in use, containing information about systems, ownership, substantive programme supported, and their relationship with the ICT strategic plan.

28. *The UNFCCC Administration partially accepted recommendation 4 and stated that this is in part covered in the Policy & Procedures for Records & Archives document (B/2007/2-September 2007). It also planned this year to complete the "engagement model" for Information Service and all concerned programmes. This model documents all key roles and responsibilities, all IT projects and processes' ownership. In addition, it is envisioned that the new technical committee will address the development of standard processes and controls for the secretariat at a deeper technical level to complement the policy. Recommendation 4 remains open pending development of standard process controls for managing information systems.*

29. *The UNFCCC Administration accepted recommendation 5 and stated that work is under way to assess all systems/applications currently in operation in the Secretariat. It also stated that under the current timeline, the resulting centralized repository for all systems/applications will be in place by July 2010 and that the information architecture will be developed for the secretariat by the end of 2010. Recommendation 5 remains open pending implementation of an information architecture plan, and the creation of a centralized repository of all applications in use, containing information about systems, ownership, substantive programmes supported, and their relationship with the ICT strategic plan.*

C. ICT Investments

30. UNFCCC has not adopted or implemented a standard methodology for the formulation, review and approval of ICT projects or ICT initiatives. Neither was a standard project management methodology (such as Prince2 or PM-BOK) adopted. In this situation, there is also no systematic analysis of costs and benefits of ICT initiatives.

31. In the absence of a standard approach to analyzing and evaluating ICT projects and initiatives, the value of ICT contribution to the substantive programmes cannot be easily determined. This may lead to financial resources not being aligned with UNFCCC's goals.

Recommendation 6

(6) UNFCCC should: (a) Define a standard methodology to prepare, review, and approve ICT projects and initiatives; (b) Introduce a cost-benefit analysis for ICT projects and initiatives; (c) Adopt a standard ICT project management methodology; and (d) Train relevant staff in the procedures of developing ICT initiatives.

32. *The UNFCCC Administration accepted recommendation 6 and stated that as part of the IT governance roadmap assessment, it has already been recognized that IT projects would benefit by closer alignment with the Prince 2 project management standard. Preparation for its adoption by the secretariat is underway and preliminary training has already been provided to lead staff. Recommendation 6 remains open pending receipt of documentation that defines a standard methodology for ICT projects and the formal adoption of a project management methodology. UNFCCC should also provide OIOS with evidence of training provided to relevant staff on procedures for developing ICT initiatives.*

D. ICT Operations

Business impact analysis and risk assessment

33. UNFCCC conducted a business impact analysis (BIA) which identified the mission-critical activities (MCAs) and their dependencies on services provided by Information Services. The BIA defined the maximum tolerable outage for each MCA. The BIA was followed by a risk assessment which focused on business continuity capabilities of Information Services. Specifically, the risk assessment addressed the "Top 10" systems, namely, those systems that support the most time-critical activities, depending on Information Services-delivered systems and infrastructure.

34. OIOS welcomed the completion of a risk assessment, and noted several additional risks related to the continuity of ICT operations. These risks are further elaborated in the following paragraphs.

Monitoring and self-assessing ICT operations

35. UNFCCC developed a catalogue of ICT services, which although not yet complete, detailed service availability parameters. At the same time, however, ICT metrics have not been defined, and no self-assessment procedures and mechanisms have been introduced. In addition, historic risk trends and events that affect ICT performance were not monitored.

36. In the absence of metrics and monitoring process, performance weaknesses may go undetected. Conversely, positive performance cannot be tracked and recognized. Additionally, controls to mitigate risks may not perform as intended, or might not address risks altogether.

Recommendations 7 to 9

The UNFCCC should:

(7) Define ICT metrics and develop standard procedures for consistent monitoring and reporting.

(8) Implement mechanisms to track historical risk trends and events, and develop procedures to record follow-up actions.

(9) Develop a self-assessment process of ICT performance, and take remedial actions when warranted.

37. *The UNFCCC Administration accepted recommendation 7 and stated that the current edition of the Information Service catalogue provides benchmarks for service delivery which will be refined as data becomes available into a systematic procedure and method. Recommendation 7 remains open pending receipt of documentation showing the defined metrics and procedures for consistent monitoring and reporting.*

38. *The UNFCCC Administration accepted recommendation 8 and stated that it will review and address the risk assessment report (ref L1-07:0004) submitted by the consultant company Combitech AB in March 2007. Additionally, this report will be incorporated into the ongoing process of implementing an Information Security Management System (ISMS) for the UNFCCC COP 15 in Copenhagen and the Secretariat. Recommendation 8 remains open pending implementation of procedures to track and follow up on historical risk trends and events.*

39. *The UNFCCC Administration accepted recommendation 9 and stated that the results of the first ICT user satisfaction survey were presented to the Secretariat's management committee in 2008. This survey assessed the ICT infrastructure and support services provided to UNFCCC users at the Secretariat Headquarters. Remedial action to address concerns, especially as they relate to printing and copying was completed in the 1st quarter of 2009. The next survey is planned for November 2009. UNFCCC further stated that for other ICT services*

provided by Information Services, the internal control mechanisms are planned to be outlined in the information service catalogue including its monitoring and evaluation reporting processes. Recommendation 9 remains open pending receipt of documentation showing that a process of performance assessment and remedial action has been established.

Managing ICT service requests and problem resolution

40. The provision of ICT support services is regulated and documented by a policy, service and operational level agreements. However, these agreements do not define any standard or uniform procedures for managing service desk requests and problems/errors resolution. This condition presents the risks of not resolving problems and incidents in a timely manner and increases the likelihood of their recurrence. Additionally, problems and incidents as well as their solutions should be tracked for proactively managing them.

Recommendation 10

(10) The UNFCCC should develop standard procedures for managing service desk requests and problems/errors, including mechanisms to monitor service requests against Service Level Agreements and guidelines to escalating incidents and prioritizing responses.

41. *The UNFCCC Administration accepted recommendation 10 and stated that Information Services had fully implemented the "Track IT" information system for managing the ICT service desk and ICT assets as of the start of 2009. UNFCCC further stated that as a next step, IS/ICT will gradually introduce IT service management (ITIL and ISO 20000) for its ICT infrastructure operations, system and user support services. Recommendation 10 remains open pending receipt of standard operating procedures for the Track IT information system.*

ICT staff training

42. While ICT job descriptions exist at UNFCCC, no individual training plans for ICT staff were prepared. This may lead to inadequate knowledge by staff of ICT products, services and technologies. Further, insufficient security awareness increases the risk of errors or incidents of information security breaches.

Recommendation 11

(11) UNFCCC should assess the training needs of staff based on job profiles and functional responsibilities. Based on these needs, UNFCCC should develop training plans for ICT staff, and consider business objectives and operational work plans.

43. *The UNFCCC Administration accepted recommendation 11 and stated that initial training needs for IT staff in the area of ITIL and Prince2 have been identified and have been or will be addressed in 2009/10. Further assessments for training needs based on the staff job profile and functional responsibilities will be conducted as part of the preparation of the following year's performance appraisal system. Recommendation 11 remains open pending receipt of training plans for ICT staff.*

Change management and user acceptance tests

44. When changes are made to information systems, best practices require that a structured process be followed. The process includes standardized and uniform procedures of implementing changes to systems, followed by structured and documented tests by users that are performed before a change is accepted.

45. UNFCCC did not have standardized and uniform procedures for managing changes to systems, nor for user acceptance testing. In this situation, there was a risk of: (a) inadequate recording of a change to systems; (b) introducing unauthorized changes to systems, including mission-critical system; (c) insufficient control over emergency changes; and (d) inadequate allocation of resources to the change process, and potentially in its aftermath.

Recommendation 12

(12) UNFCCC should develop standard change management procedures and user acceptance test procedures to ensure that: (a) Requirements for changes in systems are recorded and tracked even if eventually rejected; (b) Changes are recorded throughout the complete life-cycle of systems; and (c) Acceptance and approval of changes to systems are adequately documented.

46. *The UNFCCC Administration accepted recommendation 12 and stated that it planned during the course of 2009, to complete the engagement module under the IT governance scheme with all programmes, which will include standard change management and user acceptance testing procedures. The new procedures are expected to be adopted by the ITMC by mid-2010. Recommendation 12 remains open pending implementation of change management and user acceptance test procedures.*

E. ICT Security

Need to develop information security policies and procedures

47. UNFCCC issued guidelines on the usage and management of ICT network resources. These guidelines defined basic terms of reference regarding: a) responsibilities of the Information Services programme; b) user responsibilities; c) network resources/services provided by Information Services; d) possible security threats and mitigation procedures; and e) conventions on

UNFCCC network account credentials. While these guidelines represented a first positive step in managing important aspects of information security, a more comprehensive approach is needed to ensure UNFCCC can adequately identify risks, and corresponding safeguards. In this regard, the results of the audit highlighted the following control weaknesses:

- (a) No ICT security policy had been issued;
- (b) A dedicated ICT security committee had not been created to enable representatives from the business and technical areas to define requirements, establish priorities, and monitor their implementation;
- (c) No dedicated resources had been identified for ICT Security. Neither was a post provided for this function;
- (d) Data classification policy and criteria had not been defined;
- (e) Procedures for ICT security incident detection, reporting and investigation had not been developed.
- (f) No awareness programmes on ICT risks had been implemented.

Network security

48. OIOS conducted vulnerability security tests of the UNFCCC's network at the Bonn Headquarters. The results of the test revealed only a limited number of low or medium risk vulnerabilities. Notwithstanding, the following risks need to be addressed:

- (a) No regular interval vulnerability scanning of the network is performed; and
- (b) A Radio Frequency (RF) traffic link between the two UNFCCC main locations in Bonn, Germany was not secure.

49. The main risks presented by the above conditions are exposure of data and information assets to loss, unauthorized access, use and manipulation.

Recommendations 13 to 17

The UNCCC should:

(13) Develop and formalize an ICT security policy, and establish a dedicated committee comprising representatives from the substantive and technical areas of the Organization.

(14) Develop policies and procedures for: (a) data classification; (b) ICT security incident detection, reporting and investigation; and (c) ICT training and awareness.

(15) Secure the radio frequency traffic link between the two UNFCCC main locations in Bonn, Germany.

(16) Establish a procedure requiring periodic vulnerability scanning of the network, the review of its results, and the implementation of adequate mitigating controls.

(17) Establish a dedicated post for ICT security. Pending the establishment of the post, UNFCCC should ensure that current staff assigned to network administration implements compensating controls, such as monitoring of specialized mailing lists of known vulnerabilities of the software and devices installed at UNFCCC.

50. *The UNFCCC Administration accepted recommendation 13 and stated that in coordination with Advisory Committee on systems (ISAW) and the Information Communication Technology Committee, information services is in the process of implementing an information security management system (ISMS) that will be aligned towards the international ISO standard for information security management (ISO27000) for both UNFCCC conference and headquarter operations. Recommendation 13 remains open pending development and formalization of an information security policy.*

51. *The UNFCCC Administration accepted recommendation 14 and stated that Information Services intended to implement a SecureAware Portal that will enhance the Secretariat's ISMS process including user awareness on security policies. The implementation will include a formal training workshop for those IT staff using the system in the Secretariat. Recommendation 14 remains open pending development of policies and procedures for: (a) data classification; (b) ICT Security incident detection, reporting and investigation; and (c) ICT training and awareness.*

52. *The UNFCCC Administration accepted recommendation 15 and stated that the 2-mbits radio link between the two UN locations in Bonn is targeted to be replaced by September 2009 with a secure dedicated data-communication link. Recommendation 15 remains open pending receipt of documentation confirming the implementation of a secure dedicated data communication link between the two UN locations in Bonn.*

53. *The UNFCCC Administration accepted recommendation 16 and stated that during the OIOS audit in November 2008, a Nessus scan report was submitted and it is the intention of Information Services to maintain its application for consistent reporting. Recommendation 16 remains open pending receipt of documented procedures for periodic vulnerability scanning of the network and the review of results.*

54. *The UNFCCC Administration accepted recommendation 17 and stated that the issue of the dedicated post will be reviewed and terms of reference prepared to be considered during the next biennium. Pending this, compensating controls*

will be applied by the IS/ICT team by October 2009. Recommendation 17 remains open pending receipt of documentation describing the compensating controls implemented.

Security of mobile devices

55. OIOS noted that data on mobile computers was not protected, and hard drives were not encrypted. These conditions exposed the Organization to the risk of data loss.

Recommendation 18

(18) UNFCCC should define and implement more stringent security measures (e.g. hard-drive encryption) for mobile computers.

56. *The UNFCCC Administration accepted recommendation 18 and stated that the issue is to be addressed during the migration to the new desktop operating system which has already started (move to Windows XP operating systems) and will be completed by December 2009.* Recommendation 18 remains open pending receipt of documentation confirming the implementation of more stringent security measures for mobile computers.

Business continuity

57. UNFCCC drafted a business continuity policy and a strategy for the ICT infrastructure and critical information services. However, while these initial documents envisaged the development of detailed solutions, plans, and procedures for escalation and crisis management, the latter have not yet been completed.

58. In addition, draft terms of reference have been issued for the “Business Continuity Group”, with the mandate to act as a steering group to:

- (a) Establish and ensure the effective implementation of the plan;
- (b) Ensure the introduction and implementation of the necessary organizational, technical and budgetary arrangements required to establish and implement a business continuity management programme; and
- (c) Take other actions, as required, in relation to business continuity management and risk management within the UNFCCC Secretariat.

Recommendations 19 to 21

The UNCCC should:

(19) Formalize its business continuity policy and strategy.

(20) Formalize the terms of reference of the Business Continuity Group, and implement adequate procedures to support its function.

(21) Complete its business continuity system with the development of detailed: (a) Business continuity solutions; (b) Business continuity plans; (c) Escalation and crisis management; (d) Maintenance, testing and exercising procedures; and (e) Training and awareness programmes for staff members.

59. *The UNFCCC Administration accepted recommendation 19 and stated that the business continuity policy and strategy in relation to ICT infrastructure and critical information systems will be completed following the formalization of the terms of reference of the business continuity group. Recommendation 19 remains open pending formalization of a business continuity policy and strategy.*

60. *The UNFCCC Administration accepted recommendation 20 and stated that the current terms of reference of the business continuity group will be reviewed following the implementation of the IT governance framework, especially in relation to the creation of the IT Management Committee. Recommendation 20 remains open pending receipt of formalized terms of reference for the business continuity group.*

61. *The UNFCCC Administration accepted recommendation 21 and stated that despite the increased number of intergovernmental meetings in 2009, action has been completed to institute solutions to address immediate continuity requirements of priority systems, such as support for International Transaction Log (ITL). To fully implement a business continuity system for the organization, the Secretariat's Business Continuity Group (BCG) will need to address all other components needed including financial resources. UNFCCC envisages that the work of the BCG will be continued in 2010. Recommendation 21 remains open pending development of a business continuity system.*

V. ACKNOWLEDGEMENT

62. We wish to express our appreciation to the Management and staff of UNFCCC for the assistance and cooperation extended to the auditors during this assignment.

ANNEX 1

STATUS OF AUDIT RECOMMENDATIONS

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
1.	UNFCCC should formalize its ICT Governance model by completing the September 2008 due diligence review.	Governance	High	0	Documentation of a formalized ICT Governance Module.	August 2009
2.	Following the formalization of an ICT governance model, UNFCCC should establish an ICT Strategic Committee, with a mandate to ensure that (a) all programmes and services are adequately represented; (b) the decision-making process is based on clear terms of reference; (c) performance evaluation processes and criteria are defined; and d) an ICT Strategy is developed.	Governance	High	0	The implementation of a IT management committee and the documentation of an ICT strategy.	2010
3.	UNFCCC should review its ICT planning document to ensure that performance indicators adequately express a measurement of the activities monitored.	Governance	Medium	0	Receipt of planning documentation that includes performance indicators as a measurement of activities monitored.	March 2010
4.	UNFCCC should develop standard process controls for managing the information systems, requiring the definition of: (a) Key roles and responsibilities; (b) Process ownership; (c) Templates for data collection and reporting; (d) Criteria and procedures for quality assurance and continuous	Governance	Medium	0	The development of standard process controls for managing information systems.	December 2010

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
	improvement.					
5.	UNFCCC should complete the development of its information architecture plan, and create a centralized repository of all applications in use, containing information about systems, ownership, substantive programme supported, and their relationship with the ICT strategic plan.	Information Resources	Medium	O	The implementation of an information architecture plan and the creation of a centralized repository of all applications in use, containing information about systems, ownership, substantive programmes supported, and their relationship with the ICT strategic plan.	December 2010
6.	UNFCCC should: (a) Define a standard methodology to prepare, review, and approve ICT projects and initiatives; (b) Introduce a cost-benefit analysis for ICT projects and initiatives; (c) Adopt a standard ICT project management methodology; and (d) Train relevant staff in the procedures of developing ICT initiatives.	Governance	Medium	O	Documentation that defines a standard methodology for ICT projects and the formal adoption of a project management methodology. UNFCCC should also provide OIOS with evidence of training provided to relevant staff on procedures for developing ICT initiatives.	December 2010
7.	The UNFCCC should define ICT metrics and develop standard procedures for consistent monitoring and reporting.	Governance	Medium	O	Documentation which shows defined metrics and procedures for consistent monitoring and reporting	July 2010
8.	The UNFCCC should implement mechanisms to track historical risk trends and events, and develop procedures to record follow-up actions.	Governance	Medium	O	The implementation of procedures to track and follow up on historical risk trends and events.	May 2010
9.	The UNFCCC should develop a self-assessment process of ICT	Governance	Medium	O	Documentation showing that a process of performance assessment and	2010

Recom. no.	Recommendation	Risk category	Risk rating	C/O ₁	Actions needed to close recommendation	Implementation date ²
	performance, and take remedial actions when warranted.				remedial action has been established.	
10.	The UNFCCC should develop standard procedures for managing service desk requests and problems/errors, including mechanisms to monitor service requests against Service level Agreements and guidelines to escalating incidents and prioritizing responses.	Governance	Medium	O	Standard operating procedures for the Track IT information system.	May 2010
11.	UNFCCC should assess the training needs of staff based on job profiles and functional responsibilities. Based on these needs, UNFCCC should develop training plans for ICT staff, and consider business objectives and operational work plans.	Human Resources	Medium	O	Training plans for ICT staff.	March 2010
12.	UNFCCC should develop standard change management procedures and user acceptance test procedures to ensure that: (a) Requirements for changes in systems are recorded and tracked even if eventually rejected; (b) Changes are recorded throughout the complete life-cycle of systems; and (c) Acceptance and approval of changes to systems are adequately documented.	Governance	Medium	O	The implementation of change management and user acceptance test procedures.	July 2010
13.	The UNFCCC should develop and formalize an ICT security policy, and	Governance	High	O	The development and formalization of an Information Security Policy.	June 2010

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
	establish a dedicated committee comprising of representatives from the substantive and technical areas of the Organization.					
14.	The UNFCCC should develop policies and procedures for: (a) data classification; (b) ICT security incident detection, reporting and investigation; and (c) ICT training and awareness.	Governance	Medium	O	The development of policies and procedures for: (a) data classification; (b) ICT Security incident detection, reporting and investigation; and (c) ICT training and awareness.	June 2010
15.	The UNFCCC should secure the radio frequency traffic link between the two UNFCCC main locations in Bonn, Germany.	Information Resources	Medium	O	Documentation confirming the implementation of a secure dedicated data communication link between the two UN locations in Bonn.	September 2009
16.	The UNFCCC should establish a procedure requiring periodic vulnerability scanning of the network, the review of its results, and the implementation of adequate mitigating controls.	Governance	Medium	O	Documented procedures for periodic vulnerability scanning of the network and the review of results.	July 2009
17.	The UNFCCC should establish a dedicated post for ICT security. Pending the establishment of the post, UNFCCC should ensure that current staff assigned to network administration implements compensating controls, such as monitoring of specialized mailing lists of known vulnerabilities of the software and devices installed at UNFCCC.	Human Resources	Medium	O	Documentation describing the compensating controls implemented.	October 2009 for compensating controls March 2010 for ICT security post.

Recom. no.	Recommendation	Risk category	Risk rating	C/O ¹	Actions needed to close recommendation	Implementation date ²
18.	UNFCCC should define and implement more stringent security measures (e.g. Hard-drive encryption) for mobile computers.	Information Resources	Medium	O	Documentation confirming the implementation of more stringent security measures for mobile computers.	December 2009
19.	The UNFCCC should formalize its business continuity policy and strategy.	Governance	High	O	The formalization of a business continuity policy and strategy.	July 2010
20.	The UNFCCC should formalize the terms of reference of the Business Continuity Group, and implement adequate procedures to support its function.	Governance	Medium	O	Formalized terms of reference for the Business continuity group.	March 2010
21.	The UNFCCC should complete its business continuity system with the development of detailed: (a) Business continuity solutions; (b) Business continuity plans; (c) Escalation and crisis management; (d) Maintenance, testing and exercising procedures; and (e) Training and awareness programmes for staff members.	Governance	Medium	O	The development of a business continuity system.	September 2010

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