UNITED NATIONS NATIONS UNIES

Office of Internal Oversight Services
Internal Audit Division

AUD: AA/UNEP (001/2007) 1 February 2007

TO: Mr. Achim Steiner, Executive Director
United Nations Environment Programme

FROM: Corazon Chavez, Officer-in-Charge
Internal Audit Division, Geneva and Nairobi
Office of Internal Oversight Services (OIOS)

SUBJECT: **Audit of UNEP Secretariat to the Convention on Biological Diversity, Information Technology Controls (AA2006/220/05)**

1. I am pleased to submit the final report on the audit of UNEP Secretariat to the Convention on Biological Diversity, Information Technology Controls, which was conducted in Montreal, Canada, in July 2006, by Mr. Obin Silungwe. The main audit results were discussed during the exit conference held on 21 July 2006 and subsequent correspondence and meetings held between July and November 2006 with the Executive Secretary of the Secretariat to the Convention on Biological Diversity. A draft of the report was shared with the Deputy Executive Director in December 2006, whose comments, which were received in January 2007, are reflected in the attached final report, in italics.

2. I am pleased to note that the audit recommendations contained in this final report have been accepted and that UNEP has outlined the action plan for the implementation of these recommendations and the ones previously raised in AA2003/220/02. The table in paragraph 30 of the report identifies those recommendations, which require further action to be closed. I wish to draw to your attention that OIOS considers all the recommendations to be of critical importance.

3. I would appreciate if you could provide Mr. C. F. Bagot with an update on the status of implementation of the audit recommendations not later than 30 May 2007. This will facilitate the preparation of the twice-yearly report to the Secretary-General on the implementation of recommendations, required by General Assembly resolution 48/218B. In accordance with General Assembly resolution A/RES/59/272, the Secretary-General should ensure that the final audit report in its original version is, upon request, made available to any Member state, who may make it public.

4. Please note that OIOS is assessing the overall quality of its audit process. I therefore kindly request that you consult with your managers who dealt directly with the auditors, complete the attached client satisfaction survey form and return it to me.

5. I would like to take this opportunity to thank you and your staff for the assistance and cooperation extended to the audit team.

Attachment: final report and client satisfaction survey form

cc: Mr. A. Djoghlaf, Executive Secretary, SCBD (by e-mail)
Mr. O. De Munck , Computer Information Systems Officer, SCBD (by e-mail)
Mr. J. Childerley, Chief, Oversight Support Unit, UN Department of Management (by e-mail)
Mr. S. Goolsarran, Executive Secretary, UN Board of Auditors (by e-mail)
Mr. Thierry Rajaobelina, UN Board of Auditors (by e-mail)
Mr. M. Tapio, Programme Officer, OUSG, OIOS (by e-mail)
Ms. K. Autere, Audit Focal Point, UNEP (by e-mail)
Mr C. F. Bagot, Chief, Nairobi Audit Section, IAD, OIOS (by e-mail)
Mr. O. Silungwe, Auditor-in-Charge, IAD, OIOS (by e-mail)
Ms. J. Ogira, Auditing Assistant, Nairobi Audit Section, IAD, OIOS (by e-mail))

UNITED NATIONS NATIONS UNIES

Office of Internal Oversight Services
Internal Audit Division

Audit Report

Audit of UNEP Secretariat to the Convention on Biological Diversity, Information Technology Controls (AA2006/220/05)

Report date: 1 February 2007

Auditor: Obin Silungwe

UNITED NATIONS NATIONS UNIES

Office of Internal Oversight Services
Internal Audit Division

Audit of UNEP Secretariat to the Convention on Biological Diversity, Information Technology Controls (AA2006/220/05)

EXECUTIVE SUMMARY

In July 2006, OIOS conducted an audit of the UNEP Secretariat to the Convention on Biological Diversity (SCBD) Information Technology (IT) Controls in Montreal, Canada. This audit was a follow- up to its general audit of SCBD in February 2006 (AA2006/220/03), undertaken to look in more detail at controls over e-mails, within the context of overall arrangements for control of Information Technology.

The audit concluded that existing controls were effective at preventing external unauthorised access, but arrangements to prevent and / or detect unauthorised internal access needed to be strengthened. In particular, UNEP is requested to develop policies and procedures to guide its outposted offices in their use of IT, which include arrangements for prevention and detection of unauthorised accesses to computer systems. OIOS would like to thank SCBD IT staff for the level of co-operation extended to the audit team and for actions taken before, during, and after the audit, to address IT issues identified. OIOS is pleased to note that the audit recommendations have been accepted and UNEP has outlined the action plan for the implementation of these recommendations and the ones previously raised in AA2003/220/02.

Governance

OIOS raised a number of recommendations in its report on UNEP IT management (AA 2003/220/02 dated December 2004), including arrangements for IT governance and the need to develop policies and procedures to guide UNEP out posted offices in their use of IT. These recommendations were still open at the time of the audit, and weaknesses in the IT governance of SCBD are linked to the absence of timely implementation of these recommendations. OIOS would like to encourage UNEP to finalise implementation of these recommendations.

Information Security

Adequate physical security and data recovery arrangements were in place and needed to be supplemented by strengthening arrangements to cope with a serious hardware or software failure. In the opinion of OIOS, UNEP, in developing its IT policies should strengthen procedures dealing with the recording and monitoring of system administration access rights given to staff, and strengthen the capability for detecting and reporting computer security violations.

Asset Management

Recommendations made in OIOS' audit in February 2006, in connection with inventory and asset management were in the process of being implemented. OIOS made additional recommendations in this report to strengthen controls over movement and treatment of IT hardware and data, especially in relation to the office of the head of an organisation.

February 2007

TABLE OF CONTENTS

I. INTRODUCTION

1. This report discusses the results of an OIOS audit of the UNEP Secretariat to the Convention on Biological Diversity (SCBD) Information Technology (IT) Controls, which was carried out in July 2006 in accordance with the International Standards for the Professional Practice of Internal Auditing.

2. By an agreement of the world leaders at the Earth Summit in Rio de Janeiro in 1992, the Convention on Biological Diversity was formed to ensure conservation of biological diversity, sustaining use of its components, and the fair and equitable sharing of the benefits from the use of genetic resources. It entered into force on 29 December 1993 with current participation of 190 Parties and is governed by a Conference of Parties supported by a Secretariat that is housed by UNEP in Montreal, Canada.

3. The Secretariat is headed by an Executive Secretary at the ASG level and is supported by 42 Professional (P) and 29 General Service (GS) staff. Before January 2006, SCBD Information Technology section was part of the Implementation and Outreach Division. The IT Section consisted of three professionals, and two GS staff reporting to the Programme Officer, Clearing House Mechanism and the Principal Officer, Implementation and Outreach Division. From January 2006 the computer activities were part of Outreach and Major groups, the head of which was vacant at the time of the audit.

4. The Parties to the Convention have established trust funds to meet the costs of administering the Convention, including the costs of the Secretariat. Collected contributions for 2005 amounted to US$16 million. As explained in its report on UNEP Information Technology Management (AA 2003/220/02), UNEP IT costs are not separately identified and monitored.

5. OIOS previously audited SCBD in February 2006 (AA2006/220/3), and Information Technology findings in that report were the main focus of this audit. The main audit results were discussed during the exit conference held on 21 July 2006 and subsequent correspondence and meetings held between July and November 2006 with the Executive Secretary of the Secretariat to the Convention on Biological Diversity. A draft of the report was shared with the Deputy Executive Director in December2006, whose comments, which were received in January 2007, are reflected in the attached final report, in italics. OIOS is pleased to note that the recommendations have been accepted and UNEP has outlined the action plan for the implementation of these recommendations and the ones previously raised in its IT Management report (AA2002/220/02).

II. AUDIT OBJECTIVES

6. The overall objective of the audit was to advise the Executive Secretary, SCBD on the adequacy of controls over Information Technology activities. This included assessing whether:

(a) roles and responsibilities for IT activities had been defined; and,
(b) the internal control systems for IT activities were adequate.

III. AUDIT SCOPE AND METHODOLOGY

7. The proposed audit focussed on activities from January 2005 to June 2006. The audit activities included a review and assessment of internal control systems, interviews with staff, analysis of applicable data and a review of the available documents and other relevant records.

8. The scope was restricted to general controls over the IT environment and office automation applications, excluding IMIS and communication facilities.

IV. AUDIT FINDINGS AND RECOMMENDATIONS

A. Governance

(a) Oversight of ICT

9. ST/SGB/2003/17, dealing with the Information and Communications Technology Board (ICTB) directed that all departments and Offices Away from Headquarters should create internal or local information and technology groups or committees following the pattern of the ICTB. In line with this, OIOS recommended in its audit of UNEP Information Technology (IT) Management (AA 2003/220/02 dated December 2004) that UNEP should establish a local Information and Communications Technology Committee to ensure that;

a) UNEP strategies are aligned with the overall objectives of the United Nations Secretariat;
b) Information on departmental systems, resources and assets is maintained and updated on a regular basis;
c) Existing systems are reviewed, to confirm their cost effectiveness, and
d) Standard methodologies are developed and consistently used for IT projects.

10. OIOS was also of the opinion that Convention Secretariats and larger UNEP offices outside of Nairobi may benefit from having their own information technology committees to deal with local issues and to provide a more structured interface with any UNEP wide Committee that might be established. This matter should be addressed as part of the UNEP wide recommendation, which was still open at the time of the audit (AA 2003/220/02/01), and no separate recommendation is being raised.

(b) Structure, functions, roles and responsibilities

11. The line between administrative and substantive IT matters was not clearly defined and work needed to be done to define the amount of resources required to support each area. Over 70 percent of the IT professional time, as per work plans, was devoted to the substantive IT functions without any analysis of whether this was the appropriate level of resources for both administrative and substantive activities.

Recommendation:

To clarify the role of Information Technology in supporting programmatic and administrative areas, UNEP should assist the Secretariat to the Convention on Biological Diversity (SCBD) in determining the mandate, goals and objectives for IT in its programmatic and administrative areas and consider the structure, roles, responsibilities and resources required to carry out this mandate. The financial implications of these requirements will need to be also addressed (Rec. 01).

12. *UNEP accepted the recommendation and commented that it would be included in the responsibilities of the Strategic Implementation Advisory Team the Executive Director has put in place to support strengthening the management of the organisation, including its information technology and communication activities.* OIOS notes the response and will close the recommendation upon receipt of a copy of the results of the review of the mandate, goals and objectives for IT in SCBD programmatic and administrative areas and the structure, roles, responsibilities and resources required to carry out this mandate.

(c) Policies and procedures

13. At the time of the audit, and in the absence of any UNEP IT polices, SCBD did not have a formally approved set of written policies and procedures that were available to and in use by staff. In the opinion of OIOS the absence of these policies was a major contributory factor to the problems identified in this report. This problem is not restricted to SCBD. In its UNEP IT Management report (AA 2003/220/02), OIOS recommended that UNEP needed to develop IT policies and standards which provided a framework for demonstrating that UNEP was in line with United Nations standards where appropriate, and providing a framework and guidance to Divisions where and in what circumstances they can deviate from these norms, to achieve their mandates, roles and responsibilities, and evaluate whether policies and procedures are being followed. This recommendation is still outstanding and OIOS remains concerned at the risks which are presented by the absence of an adequate set of policies and procedures to guide and control IT usage. As a UNEP wide recommendation has already been raised and is still open (AA 2003/220/02/06) a separate recommendation is not being raised.

B. Data Integrity of E-mail system

(a) Monitoring e-mails

14. Paragraph 82 of the last audit report on SCBD (AA2006/220/03) commented that OIOS was also concerned to learn that staff e-mails had been monitored in the past, but was pleased to note that the practice was stopped in January 2006. SCBD took steps in January 2006 to strengthen controls over e-mail monitoring, which included restricting administrator access rights to IT staff only, combined with the implementation of a more secure version of the e-mail system. The risk of unauthorised access was therefore significantly reduced, but in the opinion of OIOS, cannot be considered eliminated without the use of detection tools. OIOS discussed with SCBD IT staff the capability for detection and the system information available, necessary to determine if monitoring of e-mails had taken place. SCBD did not undertake detection and the necessary information was not available. No conclusions could therefore be drawn about whether e-mail monitoring had actually occurred. A key element to assist SCBD in this respect would be to ensure they are able to carry out technical monitoring as envisaged by Section 8.1 of ST/SGB/2004/15 (use of information and communication technology resources and data) which states that "technical monitoring of the use of ICT resources is routinely performed for troubleshooting, diagnostics, statistical analysis and performance tuning". In the absence of such technical monitoring, the capability to detect and conclusively prove that e-mail monitoring occurred was not possible.

Recommendation:

> To ensure that the Secretariat to the Convention on Biological Diversity (SCBD) has the capability to undertake technical monitoring of its computer systems as envisaged by Section 8.1 of ST/SGB/2004/15 (use of information and communication technology resources and data), UNEP, should provide SCBD with the resources and tools for technical monitoring of the use of Information Communication Technology resources. This should including security, troubleshooting, diagnostics, statistical analysis and performance tuning (Rec. 02).

15. *UNEP accepted the recommendation and commented that it would be included in the responsibilities of the Strategic Implementation Advisory Team the Executive Director has put in place to support strengthening the management of the organisation, including its information technology and communication activities.* OIOS notes the response and will close the recommendation upon receipt of details of the resources and tools made available to SCBD for technical monitoring of the use of Information Communication Technology resources. This should include security, troubleshooting, diagnostics, statistical analysis and performance tuning.

(b) System administrator access

16. OIOS asked for details of all staff who had been granted system administrator access between January and December 2005. SCBD informed OIOS that, prior to January 2006, staff other than IT staff had been granted temporary access and one non-IT staff member had been granted longer-term administrator access. There was no documentation available detailing who had been granted such accesses, why they had been granted and who granted them. The absence of the documentation when combined with the fact that there was no technical monitoring taking place, meant that SCBD had weak controls in place for prevention of unauthorised access to e-mails in particular. Immediately upon taking up his assignment, the current Executive Secretary restricted access to IT staff exclusively and the list of IT staff having such privileges was provided to OIOS. Whilst OIOS is pleased to note the action taken, to ensure that system administrator access is only granted to those who need it, documentation should be kept explaining who has access and why, and access rights should be reviewed on a regular basis.

Recommendation:

> To ensure appropriate use and accountability for system administrator access granted, UNEP should advise the Secretariat to the Convention on Biological Diversity (SCBD) staff, on the arrangements required to document all system administrator access (temporary or otherwise) granted to staff, who granted them and the nature, rationale and extent of the access rights (Rec. 03).

17. *UNEP accepted the recommendation and commented that it would be included in the responsibilities of the Strategic Implementation Advisory Team the Executive Director has put in place to support strengthening the management of the organisation, including its information technology and communication activities.* OIOS notes the response and will close the recommendation upon receipt of details of arrangements put in place to document all system administrator access (temporary or otherwise) granted to SCBD staff, who granted them and the nature, rationale and extent of the access rights.

C. Security

(a) Physical security

18. OIOS was pleased to note that there was adequate physical security to the servers hosting intranet web servers, file servers, mail servers and backup storage. Access was restricted through a coded key to five people working in the IT Unit. Other staff members requiring access to the servers for various reasons could only do so with the approval of the IT unit. However, in the last six years, the code on the lock had only been changed twice and this could compromise the security and integrity of data and the applications. SCBD assured OIOS that the code would be changed regularly and therefore no recommendation was raised. *SCBD commented that in August 2006 the Executive Secretary realized that the password to the server room was not changed with the departure in December 2005 of the head of the IT section. He instructed the SCBD security officer to change the password and informed OIOS.*

(b) Access controls

19. Responsibility for network security was reflected in the PAS of the systems administrator. However, there was neither a written security policy for the IT facilities, nor an access rights policy and the following need to be strengthened:

a) There was no minimum requirement for the length of the password and no automatic requirement to change the password regularly;
b) When network staff leave, passwords on critical applications need to be changed;
c) No formally documented methods/ procedures were in place to detect security violations, investigate them and report the same to management;
d) No formally documented methods/ procedures were in place to monitor users in terms of access, timing, and services use;
e) There were no formally approved written guidelines for assigning permissions and privileges within applications, including arrangements for monitoring activity on sensitive applications.

Recommendation:

To ensure adequate control over access to data held on Secretariat to the Convention on Biological Diversity (SCBD) systems, UNEP should advise SCBD on the data security policy which should be followed, that includes details of roles and responsibilities, access rights, password management, and procedures for detecting and reporting security violations (Rec. 04).

20. *UNEP accepted the recommendation and commented that it would be included in the responsibilities of the Strategic Implementation Advisory Team the Executive Director has put in place to support strengthening the management of the organisation, including its information technology and communication activities.* OIOS notes the response and will close the recommendation upon receipt of a copy of the data security policy, which includes details of roles and responsibilities, access rights, password management, and procedures for detecting and reporting security violations.

(c) Back-up and recovery

21. OIOS was pleased to find that SCBD had made arrangements for backup and recovery, but these were not documented. SCBD's web and database servers were duplicated and backup copies of data were made regularly and the data stored on magnetic tapes and CD in the vault of a local commercial bank. The arrangements for data recovery could be further enhanced by drawing the current practices together into a business continuity plan which would also address hardware and software failure arising from natural disasters and / or premeditated malicious attack.

Recommendation:

> To ensure continuity of operation in the event of disasters affecting both systems and data, UNEP should advise the Secretariat to the Convention on Biological Diversity (SCBD) on the arrangements it needs to make contingency and disaster planning, and backup and recovery (Rec. 05).

22. *UNEP accepted the recommendation and commented that it would be included in the responsibilities of the Strategic Implementation Advisory Team the Executive Director has put in place to support strengthening the management of the organisation, including its information technology and communication activities. SCBD commented that it had made arrangements for backup and recovery, including the use of physical space outside of its premises for remote backups.* OIOS notes the response and will close the recommendation upon receipt of details of the arrangements for contingency and disaster planning.

D. Provision of IT services to SCBD

23. SCBD receives Internet services from a local service provider. The office network is connected to the internet provider via an optical fibre maintained by a local firm. SCBD also contracts services from commercial companies to supply IT equipment for meetings held outside the Secretariat. The contractual arrangements were assessed and found to be adequate during the last audit in February 2006.

24. OIOS was pleased to note that Service Level Agreements exist with both IT service providers guaranteeing uninterrupted transit to the internet and reports on bandwidth usage are available on line.

E. Human resources management

25. OIOS confirmed that all SCBD issues in connection with job descriptions/classifications, recruitment, training and E-PAS were either being addressed by management or the status was satisfactory as reported in the prior audit (audit of UNEP Secretariat to the Convention on Biological Diversity -AA2006/220/03).

F. Asset Management

(a) Inventory management

26. In the prior OIOS audit of UNEP Secretariat to the Convention on Biological Diversity (AA2006/220/03) OIOS made the following recommendations in connection with inventory management:

a) To ensure Secretariat to the Convention on Biological Diversity (SCBD) staff members are held accountable for the assets in their care and to monitor the movement of SCBD assets, room inventories should be maintained by both the SCBD Fund and Administration Unit and individual staff members. Implementation of this recommendation is at an advanced stage. The data base for Non Expendable Inventory which includes computer hardware and software equipment is in place with descriptions, bar code, location, purchase date and the value. The information can be sorted to locate all assets in a particular office and this will simplify the preparation of inventory cards.

b) To ensure Secretariat to the Convention on Biological Diversity staff members are clear on their responsibilities in respect of physical inventories, the Fund and Administration Unit should prepare stocktaking procedures to provide the staff members undertaking the physical inventory with guidance on what is required of them in undertaking the physical inventory and what reporting is required at the end of the exercise to assess movements of assets. This recommendation is also in the process of being implemented and is even more critical for IT equipment which is attractive and of high value. OIOS would like the guidelines to include policy on the movement of office computers between offices and outside the SCBD premises.

(b) Asset Management

27. In the prior OIOS audit of UNEP Secretariat to the Convention on Biological Diversity (AA2006/220/03), OIOS made the following recommendations in connection with asset management, both of which re in the process of being implemented, and OIOS is pleased with the progress being made:

a) To ensure Secretariat to the Convention on Biological Diversity (SCBD) does not retain or store obsolete and/or non-functioning assets, OIOS recommends that SCBD undertake an exercise to identify all obsolete and/or non-functioning assets and provide the list to the Local Property Survey Board for their approval to dispose of or write-off each.

b) To ensure Secretariat to the Convention on Biological Diversity (SCBD) has adequate procedure in place with respect to disposal of assets, SCBD should seek assistance from UNON in the creation of a policy including the disposal of assets and the treatment of income generated as the result of disposal of SCBD assets.

G. Other IT related issues

28. Whilst conducting its review of IT controls, three issues were brought to OIOS's attention, which arose as a result of the absence of a handover, and the lack of clear policy guidance in the areas concerned:

(a) In absence of a handover and no UNEP policy on this matter, or the treatment of e-mails addresses assigned to the head of an office, confusion had arisen over rights of access to the e-mails of the former Executive Secretary, required to prepare for an upcoming intergovernmental meeting and the conference of the parties of the Convention. Whilst the matter was raised and resolved by the United Nations Office of the Secretary-General, OIOS is concerned at the confusion caused because of an absence of policies in this area.

(b) UNEP had no policy guidance dealing with withdrawal of Information Technology resources from staff. In addition, there were no procedures in place to ensure that any such actions were accompanied by basic documentation explaining why it took place, on whose authority, and who was informed. As a consequence of the above, two staff members absent from office since March and April 2006, respectively, had their e-mail access withdrawn in June 2006. While the intention was to only block remote access, the setting had been inadvertently set to prevent any access. OIOS was told that the action had been taken in response to concerns about the Executive Secretary's safety and the legality of the staff member's absence. OIOS was concerned about the lack of a clear policy as a basis for the withdrawal of the access. OIOS was appreciative that e-mail access was immediately restored to the staff members when OIOS brought this matter to SCBD's attention.

(c) SCBD had no policies in place dealing with the treatment of computers, and data residing on them, when staff moved between offices. There was also no provision for the fact that some computers may contain data of a more sensitive nature than others and may require different treatment. In the absence of such policies, confusion had arisen about the movement of a computer being used in the Office of the Executive Secretary and treatment of the data residing on it. The matter was resolved internally, and OIOS confirmed that no data was copied in the physical absence of the owner, which would have been a contravention of ST/SGB/2004/15 (Use of information and communication technology resources and data).

Recommendations:

To ensure a smooth transition between incoming and outgoing heads of a UNEP office, UNEP should create handover procedures which covers how the e-mails of the head of an organisation should be viewed and treated from the standpoint of operational continuity when a change of head occurs (Rec. 06).

To provide more effective control over UNEP Information Technology resources, UNEP should issue guidance to its staff addressing the circumstances in which information technology resources may be withdrawn, movement of IT resources within the organisation and how electronically held data should be handled when staff members change offices, taking account of the sensitivity of the data on the computer (Rec. 07).

29. *UNEP accepted the recommendations and commented that they would be included in the responsibilities of the Strategic Implementation Advisory Team the Executive Director has put in place to support strengthening the management of the organisation, including its information technology and communication activities.* OIOS notes the response and will close:

- recommendation 6 upon receipt of a copy of the handover procedures which covers how the e-mails of the head of an organisation should be viewed and treated from the standpoint of operational continuity when a change of head occurs;
- recommendation 7 upon receipt of a copy of the guidance addressing the circumstances in which information technology resources may be withdrawn, movement of IT resources within the organisation and how electronically held data should be handled when staff members change offices, taking account of the sensitivity of the data on the computer.

V. FURTHER ACTIONS REQUIRED ON RECOMMENDATIONS

30. OIOS monitors the implementation of its audit recommendations for reporting to the Secretary-General and to the General Assembly. The responses received on the audit recommendations contained in the draft report have been recorded in our recommendations database. In order to record full implementation, the actions described in the following table are required:

Recommendation No.	Action Required
Rec. 01	Receipt of a copy of the results of the review of the mandate, goals and objectives for IT in SCBD programmatic and administrative areas and the structure, roles, responsibilities and resources required to carry out this mandate.
Rec. 02	Receipt of details of the resources and tools made available to SCBD for technical monitoring of the use of Information Communication Technology resources. This should include security, troubleshooting, diagnostics, statistical analysis and performance tuning.
Rec. 03	Receipt of details of arrangements put in place to document all system administrator access (temporary or otherwise) granted to SCBD staff, who granted them and the nature, rationale and extent of the access rights.
Rec. 04	Receipt of a copy of the data security policy, which includes details of roles and responsibilities, access rights, password management, and procedures for detecting and reporting security violations.
Rec. 05	Receipt of details of the arrangements for contingency and disaster planning.
Rec. 06	Receipt of a copy of the handover procedures which cover how the e-mails of the head of an organisation should be viewed and treated from the standpoint of operational continuity when a change of head occurs.
Rec. 07	Receipt of a copy of the guidance addressing the circumstances in which information technology resources may be withdrawn, movement of IT resources within the organisation and how electronically held data should be handled when staff members change offices, taking account of the sensitivity of the data on the computer.

VI. ACKNOWLEDGEMENT

31. I wish to express my appreciation for the assistance and cooperation extended to the audit team by the management and staff of the Secretariat to the Convention on Biological Diversity.

Corazon Chavez, Officer-in-Charge
Internal Audit Division, Geneva and Nairobi
Office of Internal Oversight Services