UNITED NATIONS
INTEROFFICE MEMORANDUM

NATIONS UNIES
MEMORANDUM INTERIEUR

AUD II-7-4 00723/05 21 September 2005

TO: Dr. Supachai Panitchpakdi, Secretary-General
United Nations Conference on Trade and Development

FROM: Egbert C. Kaltenbach, Director
Internal Audit Division II
Office of Internal Oversight Services

SUBJECT: **Audit of United Nations Conference on Trade and Development Information and Communications Technology Management (AE2005/340/01)**

1. I am pleased to submit the final Report on the audit of UNCTAD's Information and Communications Technology Management, which was conducted by Mr. Leonard Gauci during the second quarter of 2005.

2. A draft of the report was shared with the Director, Executive Direction and Management, UNCTAD on 8 August 2005. His comments of 2 September 2005 are reflected in this final report.

3. I am pleased to note that all of the audit recommendations contained in the final Audit Report have been accepted, and that UNCTAD has initiated their implementation. The table in paragraph 59 of the report identifies those recommendations which require further action to be closed. I wish to draw your attention to recommendations # 1 to 5, 7 to 9 and 11 to14, which OIOS considers to be of critical importance.

4. I would appreciate if you could provide me with an update on the status of implementation of the audit recommendations not later than 30 November 2005. 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.

5. 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 and return it to me.

6. Thank you for your cooperation.

Attachment: Client Satisfaction Survey

cc: Mr. Christopher B. Burnham, Under-Secretary-General, Department of Management (by e-mail)
Mr. S. Goolsarran, Executive Secretary, UN Board of Auditors
Mr. T. Rajaobelina, Deputy Director of External Audit (by e-mail)
Mr. Carlos Fortin, Deputy Secretary-General, UNCTAD (by e-mail)
Mr. Victor P. Busuttil, Director, Executive Direction and Management, UNCTAD (by e-mail)
Mr. O. Oduyemi, Chief, Administrative Service, UNCTAD (by e-mail)
Mr. M. Weidmann, Chief, Information Technology Support, UNCTAD (by e-mail)
Mr. M. Tapio, Programme Officer, OUSG, OIOS (by e-mail)
Ms. C. Chávez, Chief, Geneva Audit Section (by e-mail)
Mr. L. Gauci, Auditor-in-Charge (by e-mail)
Mr. D. Tiñana, Auditing Assisting (by e-mail)

United Nations
Office of Internal Oversight Services
Internal Audit Division II

Audit Report

Audit of United Nations Conference on Trade and Development Information and Communications Technology Management (AE2005/340/01)
Report No. E05/R13

- **Report date: 21 September 2005**
- **Auditor:** Mr. Leonard Gauci, Auditor-in-Charge

UNITED NATIONS  **NATIONS UNIES**

Office of Internal Oversight Services
Internal Audit Division II

Audit of United Nations Conference on Trade and Development Information and Communications Technology Management (AE2005/340/01)

EXECUTIVE SUMMARY

During the second quarter of 2005, OIOS conducted an audit of UNCTAD's Information and Communications Technology Management function.

The audit did not reveal major weaknesses. However a number of measures need to be taken to strengthen the governance structure over UNCTAD's overall ICT operations and to bring these in line with the policies of the United Nations Secretariat. *UNCTAD has accepted all of the recommendations and has initiated their implementation.*

Information Technology Support (ITS) within the Division of Management mainly handles operational matters and some aspects of security. UNCTAD's four substantive divisions operate specific systems that are critical to their programmes of work. These systems are maintained and run independently of UNCTAD's ITS. An IT Board has only met twice during the past two years and has largely been ineffective. Furthermore, there is no suitably qualified senior official to oversee ICT policy matters and see that these are implemented.

UNCTAD should set up an ICT committee in compliance with ST/SGB/2003/17 and should assign the functions of Chief Information Officer to a senior official. The committee would oversee all major decisions related to software applications, define system and data ownership and monitor IT-related matters. The official assigned CIO functions would report to the committee and be responsible for all of UNCTAD's ICT strategic planning, coordination and policy implementation. *OIOS is pleased to note that UNCTAD is taking immediate steps to strengthen its ICT governance through the implementation of these recommendations.*

OIOS would like to draw management's attention to the fact that systems development and other ICT activities undertaken by entities which form part of the UN Secretariat will need to comply with standards and procedures set out by the ICT Board irrespective of the source of funding.

Another critical action required of management is the implementation of a formal ICT strategy covering all aspects of ICT within UNCTAD and supporting the entity's mandates. The strategy should also reflect the global ICT policies of the UN Secretariat. *UNCTAD has taken the first steps towards the implementation of this recommendation and is in the process of discussing an ICT strategy document drafted by the Chief, ITS. The timing and details of implementation of a number of recommendations made in this report will be linked to the ICT strategy document.*

Changes to existing ITS staff resources will depend on whether the ICT strategy will indicate the need to set up a systems development function. OIOS is of the opinion that UNCTAD should first make every attempt to use applications and services that are already available through entities such as the Information Technology Service Division (ITSD) at UN Headquarters and UNOG's Information and Communication Technology Service, and to rationalize certain services, as it is planning to do with the Help Desk function. OIOS sees the introduction of individual work plans and time records as a useful tool for analyzing the adequacy of resources to carry out the tasks set out in the ICT strategy.

UNCTAD does not have a complete inventory of its ICT equipment, application software and databases. Such a list is necessary for planning purposes and to safeguard the entity's assets. OIOS came across a system that was purchased from a minor supplier and over which there are no guarantees of continued support. Such systems should be covered by an escrow agreement guaranteeing UNCTAD access to the source code if the supplier terminates system support. *Management has taken steps to address the shortcoming and will avoid a recurrence.*

The nature and scope of services that ITS is responsible to provide to users are not defined. These services should be set out in service level agreements. OIOS is also recommending the setting out of policies and criteria for the replacement of ICT equipment, a formal process to evaluate requests for modifications to systems, and the introduction of an on-line system for users to log their requests for computer equipment. The introduction of these measures should improve the level of ICT services to the user community and generate more accountability and transparency.

UNCTAD does not have a formal policy covering all aspects of IT security, including the granting and administering of access rights, and OIOS is recommending the implementation of such a policy. The network administrator is not always informed of terminated employees and consultants in order to close their e-mail account, and these accounts may still be accessed remotely via the Internet. OIOS is recommending that Human Resources Management Section is assigned responsibility to inform ITS of all terminating employees and consultants. UNCTAD is also being asked to evaluate the option of e-mail encryption and the introduction of measures that would provide tighter security over remote access. *Management is proposing to request the United Nations International Computing Centre to carry out a security policy assessment, followed by the setting up of IT security policies.*

OIOS is recommending that ITS coordinate with ITSD to implement as soon as possible the Global IT physical security policies. Management should also assess the risk of the computer room's current location, which is directly above the Palette bar, and the absence of a fireproof safe, and take appropriate action. There are no detailed plans to ensure that in the event of a major disaster UNCTAD's critical operational functions are properly recovered and become operational within acceptable timescales. OIOS is recommending that UNCTAD request the assistance of ITSD to perform an ICT security risk assessment and seek to benefit from the work already undertaken by ITSD in relation to business continuity planning. *Management is in the process of evaluating the risks and the best options for the implementation of the recommended actions.*

OIOS believes that the implementation of the recommendations set out in its report would bring the management of ICT more in line with best practice and would demonstrate management's commitment to ensuring proper control.

TABLE OF CONTENTS

I. INTRODUCTION

1. During the second quarter of 2005, OIOS conducted an audit of Information and Communications Technology management within the United Nations Conference on Trade and Development. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

2. The UNCTAD secretariat has around 400 staff members and is divided into five divisions, of which four are focused on the substantive research and technical assistance work of the secretariat, while the fifth, the Division of Management includes the Resources Management Service, the Technical Co-operation Service and the Intergovernmental Affairs and Outreach Service. In addition, a Special Programme is dedicated to dealing with issues affecting the least developed countries. The Chief, Information Technology Support, reports to the Chief, Resource Management Service within the Division of Management.

3. The findings and recommendations contained in this report have been discussed during the Exit Conference held on 8 July 2005 with the Director, Executive Direction and Management, the Programme Management Officer, Executive Direction and Management and the Chief, ITS. A draft of this report was communicated to the Director, Executive Direction and Management on 8 August 2005. Comments received on 2 September 2005 are reflected in the report in italics.

II. AUDIT OBJECTIVES

4. The main objectives of the audit were to:
   (a) Assess UNCTAD's governance and organisational structure with respect to ICT;
   (b) Determine what is required for the development of UNCTAD's strategic plan for ICT;
   (c) Assess UNCTAD's practices and plans for ICT against the global ICT strategy of the UN Secretariat; and
   (d) Identify areas of ICT that require the attention of UNCTAD's management to bring them in line with best practice.

III. AUDIT SCOPE AND METHODOLOGY

5. The four substantive divisions within UNCTAD have significant ICT responsibilities independently of ITS, and develop, implement and maintain their own application systems. In addition, several databases, applications and web sites are designed and maintained by substantive divisions and such applications are currently not controlled by ITS.

6. The review focused on the relevant areas of Information Technology controls that fall under UNCTAD. It did not examine the IT controls over individual application systems or the functionality aspects of such systems.

7. OIOS sought to obtain an understanding of the computer environment at UNCTAD (organization, systems and key performance indicators) through the completion of a questionnaire. A set of tailored audit programmes covering all the audit objectives was developed on the basis of the above and discussions with key personnel. Interviews were also held with selected managers staff from the substantive divisions. During the audit, OIOS

analysed applicable data and reviewed the available documents and other relevant records.

IV. AUDIT FINDINGS AND RECOMMENDATIONS

A. Establishing a governance structure for the UNCTAD ICT function

1. Setting up an effective governance body

8. In recent years, the governance role for ICT within UNCTAD has been assigned to the IT Board. This Board is composed of representatives from UNCTAD's Division of Management and the four substantive divisions. It is scheduled to meet twice a year but the last two meetings were held in autumn 2003 and autumn 2004.

9. The lack of activity and participation within the IT Board was confirmed during our discussions with representatives from the substantive divisions. As a result, the Board failed to serve as an effective mechanism for bringing all of UNCTAD's divisions under a common IT policy.

10. UNCTAD forms part of the Secretariat of the United Nations (ST/SGB/1997/5) and is therefore governed by the Secretary-General's bulletin "Information and Communications Technology Board" (ST/SGB/2003/17). This bulletin calls for all departments and offices away from Headquarters to establish information and communications technology Committees (ST/SGB/2003/17 para. 4.4). As a first step towards establishing an effective governance structure covering all aspects of ICT within the organization, UNCTAD should set up an ICT Committee with adequate representation from the user community. This Committee would oversee all major decisions regarding new software applications, define system and data ownership and monitor IT-related matters to see that they are in line with UNCTAD's ICT strategy.

11. Having a strong functioning ICT Committee and a well-defined governance structure for the whole of the organization's ICT would give UNCTAD a stronger voice when dealing with the Secretariat's ICT Board.

Recommendation:

- UNCTAD should set up its ICT Committee in line with the requirements of Section 4.4 of ST/SGB/2003/17. The terms of reference of the Committee should be approved by the Secretary-General of UNCTAD (Rec. 01).

Management response: *While revised ToR for UNCTAD's IT committee have been drafted and will be discussed at the next IT Board meeting, the incoming Secretary-General of UNCTAD - whose appointment commenced on 1 September - will need to be seized of the matter. Consequently, while these ToR are in line with ST/SGB/2003/17 and include functions as per ST/AI/2005/10 concerning ICT initiatives they may require some amendment once the SG has reviewed them, naturally on the understanding that any changes to them would be in line with these administrative provisions. Thus, by way of example, the chair of the ICT Committee would*

in all likelihood be the Director, Division of Management (see our comments on recommendation 2 below).
Implementation: September - October 2005.

OIOS takes note of management's response. It will keep this recommendation open pending receipt of the ICT Committee's Terms of Reference, approved by UNCTAD's SG, and minutes of the Committee's first meeting.

2. Chief Information Officer functions

12. An effective ICT Committee will be useful for carrying out the governance function, but such a body usually meets a few times a year. Corporations that have a structure similar to that of UNCTAD, i.e. a central administrative role and a number of divisions providing specialized products or services to a specific client base have adopted the CIO function to achieve a more effective governance structure.

13. Within the UN organization, General Assembly resolution 57/304, para. 4, requested the Secretary-General, *inter alia*, to make proposals on how to reflect the functions of chief information and communication technology officer of the United Nations in the organizational structure of the Organization, as suggested by the Advisory Committee on Administrative and Budgetary Questions. In response, the Secretariat stated that the Project Review Committee of the ICT Board provides the head of the information technology services division, as chair of this committee, with a strong, central authority over Information and Communication Technology initiatives in the global Organization (A/58/7 Annex IX).

14. In its report on the management of information systems in United Nations organizations, the Joint Inspection Unit recommended that the Executive Heads appoint or designate a senior official to serve as CIO (A/58/82, Recommendation 2). Depending on the size of the organization, the CIO or the official (including the chief of "an appropriate unit") who has CIO functions would report directly to the Executive Head or to the Deputy Executive Head in charge of programmes. The report also recommended that "… depending upon organization-specific circumstances, the CIO functions could be performed by an appropriate unit or, in the case of small organizations that cannot afford a CIO, by a senior official with organization-wide coordinating responsibilities as well as some IT knowledge".

15. The designation or appointment of a senior official as CIO was also recommended by the JIU to the United Nations High Commissioner for Refugees (A/59/394/Add.1 para. 19, Recommendation 7(d)). In 2004, UNHCR recruited and appointed a CIO at the D-2 level to perform the above-mentioned functions.

16. In the case of UNCTAD, ITS is not responsible for the entire scope of IT services provided by the organization. To a large extent, ITS has been carrying out a support function and approving the purchases of computer hardware. It has no control over systems that are developed, implemented and maintained within the framework of Technical Cooperation projects and project managers have no obligation to consult with or involve ITS. Consequently, ITS is not in a position, for example, to monitor the development of applications in the substantive divisions to see that this complies with the Secretariat's global ICT policies over systems

development and security standards. This could result in lack of uniformity and compatibility between systems, and potentially weak access security. From our discussions there also appears to be a lack of coordination with regard to security, back-up policies and recovery procedures, with some divisions relying on ITS, others having their own, or a combination of the two.

17. Application systems such as TRAINS, DMFAS and ASYCUDA, on which the service provided by the respective substantive division is based, are "stand-alone" systems in the sense that there is no interfacing between theses systems or with core UN application systems such as IMIS and Galaxy. OIOS agrees that UNCTAD's divisions need to retain a degree of autonomy in view of the specialized nature of their operations and their need to address quickly requests from their clients. However, there would be a significant improvement in governance if certain functions that apply across UNCTAD as a whole are managed by one unit, such as ITS, which in turn would report directly to someone assigned the functions of a CIO. This set-up would have its advantages when it comes to planning and coordination, would make it easier to ensure systems compatibility and standardization, and makes compliance with Secretariat-wide policies more manageable.

18. While it may not be feasible, at this stage, for UNCTAD to establish a full-time post for CIO, the functions of this role should be defined and assigned to a suitably-qualified senior official. In broad terms, this official would coordinate the policy and direction for all ICT matters and discuss these at the senior management level, namely the Secretary-General, Deputy Secretary-General, and the directors of the divisions. The other major benefit is that a CIO will be in a position to identify areas where efficiencies can be achieved. This person would report to the ICT Committee. A list of specific responsibilities that may be assigned to the CIO function is attached at Annex A.

Recommendation:

- UNCTAD should:
  (a) Assign the functions of Chief Information Officer (CIO) to a suitably-qualified senior official with responsibility for all its ICT planning, coordination and policy implementation; and
  (b) Define the ICT-related functions that fall under the responsibility of the CIO and administered by Information Technology Support (Rec. 02).

Management response: *The draft vacancy announcement for the position of Director, Division of Management, which has been cleared by the incoming SG of UNCTAD, reflects this recommendation. Implementation: January 2006.*

OIOS will keep this recommendation open pending the receipt of a copy of the vacancy announcement and the new Director for the Division of Management's terms of reference.

B. Implementing an ICT strategy for UNCTAD

1. ICT Strategy

19. UNCTAD does not have a strategy for information technology systems that is approved at the highest level. Such a plan is necessary to ensure that the entity has the right systems to support its mandate and is able to provide the best service to its clients.

20. The absence of a comprehensive ICT strategy that is linked to management strategy and is subject to periodic review and updating to take into account technological developments has resulted in instances where ITS was not able to meet demands of a technical nature from the substantive divisions and the latter had to resort to external sources; for example in areas of wireless solutions, remote e-mail access and video conferencing.

21. ITS prepares a budget proposal for the forthcoming biennium on the basis of a medium-term work plan and the requirements submitted by the divisions. The latter are basically for hardware requirements. OIOS is of the opinion that budgets and funding resources would be applied to best effect if budgeting were directly based on the ICT strategy for the whole entity.

22. OIOS is pleased to note that an "ICT Business Strategy for UNCTAD" has now been drafted by the Chief, ITS and encourages a fast timeline for its review by management to ensure it adequately covers the services to be provided within UNCTAD as well as those to external clients, and include details of deliverables, timing and resource requirements.

Recommendation:

- UNCTAD should request ITS to submit for the ICT Committee's review and approval a rolling strategic plan for IT services and applications covering the next two biennia. Once approved by the Committee, the plan should be endorsed by the Secretary-General of UNCTAD and implemented and should serve as a basis to determine UNCTAD's ICT budget requirements for the 2008-2009 biennium (Rec. 03).

Management response: *ITS has already requested the organization of an IT Board meeting to discuss the proposed ICT strategy. In the meantime, a copy of the draft ICT business strategy document has been provided to OIOS.*
Implementation: Autumn 2005.

OIOS takes note of management's response. It will keep this recommendation open pending the receipt of a copy of the ICT strategy endorsed by UNCTAD's SG.

2. Compliance with the Secretariat's global ICT policies

23. The absence of a strategy for ICT that takes into consideration the services available through other UN entities such as UNOG and the Secretariat may result in duplication. In fact, many non-standard and duplicative systems, funded from extrabudgetary resources, have entered the Secretariat's ICT resource portfolio.

24. To ensure the coherent and coordinated global management of ICT initiatives across departments and duty stations, SGB/2004/15 on the use of information and communication technology resources and data, and a new ST/AI titled "ICT initiatives" that will soon come into effect, promulgate very broad and inclusive definitions of what constitutes an ICT resource and an ICT initiative, irrespective of how this is funded. ST/SGB/2004/15 defines ICT resource as "Any tangible or intangible asset capable of generating, transmitting, receiving, processing, or representing data in electronic form, where the asset is owned, licensed, operated, managed, or made available by, or otherwise used by, the United Nations". (Section 1 (b)). An ICT initiative will consist of "Any project or activity, irrespective of its source(s) of funding or its cost, that will result in a new or modified ICT resource."

25. In addition to all networking, computing, ICT consulting and internal expenditures of staff resources related to an ICT initiative, telephone systems, audio equipment, electronic interpretation support, cell phones, building automation, security and access control and CCTV would also fall under the definition of ICT resource, and as such, any initiative related to them will need to be managed in accordance with these instructions.

26. The report of the Secretary-General on the ICT strategy for the Secretariat worldwide states that "in line with the broad objectives of the strategy, all ICT investments need to generate tangible returns" (A/57/620, paragraph 31). It also calls for the use of mandatory cost-benefit analyses as a prerequisite for the development of all new systems and for the initiation of ICT-related projects to ensure a consistent approach and returns on investment (A/57/620, paragraph 77).

27. ST/SGB/2003/17 established the Project Review Committee "to apply uniformly the standards decided upon by the Information and Communications Technology Board to information and communications technology initiatives within the Organization and to recommend whether such initiatives should proceed" (ST/SGB/2003/17, paragraph 5.2). The PRC is fully operational and meets as needed to review High Level Business Cases for projects costing more than $200K.

28. ITS did not undertake any major software development projects during the past four years. However, it has not been consulted or involved in ICT initiatives within the substantive divisions and is not in a position to say whether these conform to those promulgated by the ICT Board. The Chief, Programme on Debt Management and Financial Analysis (DMFAS), for example, affirmed that although they do apply systems development standards and methodologies, they work independently of the ICT Board and the PRC.

29. UNCTAD should have a mechanism that will provide senior management with assurance that methodologies in conformity with those promulgated by the ICT Board are being applied for

project management, system design and testing. In addition to conforming to Secretariat regulations, this would reduce the risk of systems being delivered late and over budget, and of inadequate security features.

Recommendations:

- UNCTAD should see that the future strategic plan for its overall IT services and applications is aligned with the global ICT strategy of the United Nations Secretariat and establish a mechanism to ensure it remains in compliance with the global ICT policies of the Secretariat (Rec. 04).

- Once established, UNCTAD's ICT Committee should monitor all systems development within UNCTAD, irrespective of the source of funding, and ensure this follows the methodologies, standards and procedures set out by the ICT Board and Project Review Committee (Rec. 05).

Management response: *Both recommendations are addressed in the ICT business strategy document. In particular, the UNCTAD ICT board will be responsible for approving local High Level Business Cases (HLBC), and also proposes the establishment of a project management working group to oversee software development in UNCTAD.*
Implementation: Autumn 2005 with the approval of ICT strategy.

OIOS takes note of management's response. It will keep these recommendations open pending receipt of the ICT Committee's Terms of Reference, approved by UNCTAD's SG, and minutes of the Committee's first meeting (recommendation 1), and a copy of the ICT strategy endorsed by UNCTAD's SG (recommendation 3).

3. ICT staff resources

30. ITS currently has 17.5 posts. Eight of these are at the professional level but one is on loan to another division. Over the past three years, ITS has employed the services of consultants in the area of software development and maintenance of applications at an average of 50 to 80 man-days per year. There are about 600 PCs installed.

31. ITS has been providing a service that is essentially aimed at ensuring users can access their systems without interruption, and that the integrity of data held on these systems is safeguarded.

32. The most critical factor affecting ICT resource requirements will be whether UNCTAD needs to have its own software development and maintenance function in addition to those employed by the Technical Cooperation projects or whether it will continue to provide general support and assistance to users. Such a function would be very costly to set up and maintain, and its viability will need to be backed by a return on investment analysis. Management will also need to make sure there is no duplication with services and systems that are already being provided or are available from entities such as the Secretariat's ITSD, UNOG and the United

Nations International Computing Centre (ICC). It should also seek to rationalize certain services as it is currently planning on doing by consolidating the Help Desk function with that of UNOG.

33. Obtaining new posts under the regular budget will be very difficult under current UN budgetary policies. Outsourcing to ICC may be an option, especially if the purpose is the development of new systems. However, the work to be outsourced will need to be defined and linked to the ICT strategy. Another option is the recovery of funds from the extra-budget programmes related to specific projects to finance the maintenance of systems once these have been implemented.

34. This could be an opportunity to introduce mechanisms for measuring productivity and efficiency. OIOS is of the opinion that the introduction of individual work plans and time records within ITS will help management to make an informed case for requesting additional posts, the services of consultants or funds for the outsourcing of services.

Recommendation:

- UNCTAD, ITS should introduce individual work plans and time records and use them for analyzing the adequacy of resources to carry out the tasks set out in the ICT strategy (Rec. 06).

Management response*: The e-PAS partially covers the issue of individual work plans. At the same time, it is recognized that this requires strengthening including through enhanced time management and recording.*
Implementation: Once ICT strategy is approved.

OIOS takes note of management's response. It will keep this recommendation open pending further details on the actions management will be taking to enhance time management and to determine the IT staff resources required to meet the ICT strategy objectives.

4. Support for packaged systems

35. UNCTAD currently operates a "Web content management system". This was purchased from a minor supplier and ITS does not have a copy of the source code or an agreement that in the eventuality that the supplier will no longer support the system, the source code would be made available to UNCTAD. OIOS recommended that UNCTAD should ensure that systems purchased from minor suppliers are covered by an escrow agreement guaranteeing it access to the source code if system support is terminated.

Management responded that: *"Actions have already been taken to address the issue of the mentioned source code (ITS has it). In future, ITS will ensure that source code of outsourced development is fully part of the deliverables and this would be included in the relevant contract."* OIOS takes note of management's response and considers this recommendation as implemented.

C. ICT services provided to users

1. Service Level Agreements

36. The scope of ICT services to be provided by ITS to users is not clearly defined and agreed upon. There is a "User's Computing" working group that brings together ITS management and the IT focal points from UNCTAD's various divisions. This working group is scheduled to meet three times a year. (OIOS was provided with the minutes of the last meeting held on 3 February 2005).

37. OIOS welcomes the existence of a forum that could help IT services become more client-oriented. However, the services expected of ITS should be clearly defined and formalized in service level agreements between ITS and the management of the particular user-group, including the four substantive divisions. These would take into consideration the fact that the divisions need to be oriented towards the needs of their clients, which are of a distinct and specific nature, while ITS needs to be more client-oriented towards all the components of UNCTAD. This is more important given ITS' limited resources and should help avoid situations where users expect and demand certain services that ITS is not equipped to deliver.

Recommendation:

- UNCTAD, ITS should identify all the ICT services it is requested to provide to each of the substantive divisions and the rest of the user community, and have these services and respective responsibilities defined in a service level agreement signed by ITS and the respective user group (Rec. 07).

Management response: *While currently ITS has a service catalogue which describes the portfolio of services delivered, no SLA is yet been adopted. Establishing SLAs is a two way street process requiring agreement between the user group concerned and ITS and will require several phases of discussion.*
Implementation: 2006.

OIOS takes note of management's response. It will keep this recommendation open pending the receipt of a copy of all the SLAs.

2. Inventory of hardware and systems

38. UNCTAD has a formal policy for the replacement of desktop computers but there is no similar policy that sets out the criteria for replacing other items of IT equipment such as laptops, printers and scanners. In the case of technical cooperation projects, the mandate of ITS is only to provide a technical evaluation, whereas the requirement to seek compliance with central policies is not clearly documented.

39. To ensure standardization and compatibility of all items of IT equipment, the replacement of all items of such equipment should follow a set policy and be subject to a review against established criteria.

Recommendation:

- Once set up, UNCTAD's ICT Committee should establish policies and criteria for the replacement of all items of computer hardware and IT equipment within UNCTAD (Rec. 08).

Management response: *Replacement policies exist for desktop computers as well as for assignment of personal printers. Clearly, such policies can be extended to other items. It is proposed to take up the matter in the next meeting of the desktop computing working group. One observation here is to match policies with flexibility, so that undue rigidity is avoided.*
Implementation: *first half of 2006.*

OIOS takes note of management's response. It will keep this recommendation open pending the receipt of documentation setting out the policies and criteria for the replacement of all items of computer hardware and IT equipment within UNCTAD.

40. UNCTAD does not have a complete list of its IT hardware and equipment. This is partly due to difficulties in tracking IT equipment that has been allocated to consultants when their contract expires and terminating staff who are not 100 series.

41. An accurate list of IT hardware and equipment is the basis for control over the entity's ICT assets. It is also required by management to make informed decisions when ordering new equipment. Management should therefore take steps to compile and maintain a complete and up-to-date inventory of all types IT equipment within UNCTAD, showing technical details, location and user, and the installation/due replacement dates.

42. For the same reasons, OIOS is also recommending the introduction of similar procedures with regard to application software and databases so that management has a readily available list of all applications and databases in use within UNCTAD.

Recommendation:

- UNCTAD should
  (a) Request ITS to compile an inventory of computer hardware and equipment and set a database of application software and databases; and
  (b) Assign Human Resources Management Section with the responsibility of informing ITS of all employees and consultants whose contracts are expiring (Rec. 09).

Management response:
i. With the implementation of Microsoft's System Management System (SMS) in 2005/06, hardware inventory will be easier to manage and maintain. However, it will still require the implementation of improved processes in order for ITS to be aware of staff movements in a timely manner. In this light, ITS proposes implementing an identity management system data base which would, inter alia, define a unique process to create and maintain identities and accelerate the access

to organizational resources to staff members (e.g. creation/closure of a mailbox for ITS, but also for other purposes such as human resources or general services matters).
Implementation: to be defined.

ii. As far as the inventory of software is concerned, the issue is also addressed by the ICT strategy paper. This envisages giving the mandate to maintain the IT applications portfolio and address issues like assigning priorities in software development to the project management working group mentioned therein.
Implementation: depends on strategy approval and endorsement.

OIOS takes note of management's response and encourages UNCTAD to set timelines for the full implementation of these initiatives. In the meantime, OIOS recommends the immediate implementation of recommendation 09(b), at least as an interim measure. It will keep these recommendations open pending confirmation that systems for the effective management and control of computer hardware and software, and for maintaining an accurate list of user profiles are in place.

3. User support

43. Senior staff in the substantive divisions acknowledged the improvement in IT services achieved over the last few years. They also saw room for improvement especially when it comes to dealing with requests for hardware and providing, directly or indirectly, services based on state-of the-art technology. The aforementioned service delivery agreements should go some way to address this issue.

44. One remark, with which OIOS concurs, is the need for a system by means of which users can log their request for items of equipment and monitor the status of their request. The implementation of such a log should not be difficult and would also ensure more accountability and transparency in dealing with such requests.

45. The process of evaluating and implementing requests for modifications to application systems is not formalized. Changes to application systems need to be properly specified to ensure they do not adversely impact on other systems or the integrity of data. These modifications have a cost element even when performed in-house and there should be a proper evaluation to ensure that the changes are necessary and do not arise from failure on the users' part to make proper use of the application. This evaluation procedure should also result in the prioritised of modifications according to their importance.

Recommendation:

- UNCTAD, should
  (a) Set up a committee with IT and user representatives to evaluate user requests for modifications and enhancements to systems, and to prioritize such requests; and
  (b) Request ITS to implement an on-line system for users to log their requests for hardware and computer equipment, and monitor the status of their request (Rec. 10).

Management response: *The issue is partially addressed by the ICT strategy. However, the design and implementation of an on-line system will depend on software development priorities and resources.*
Implementation: To be defined

OIOS takes note of management's response. It suggests that UNCTAD sets timelines for the full implementation of the recommended actions. OIOS will keep this recommendation open pending confirmation that the recommended committee has been set-up and is functioning, and that an on-line system for users requests is operating.

D. Access security

1. General policies

46. ITS deals with aspects of an operational nature and is therefore responsible for ensuring data security within UNCTAD. For example the Division on International Trade in Goods and Services, and Commodities (DITC) uses one of the ITS servers to relay information from the TRAINS system to the database that is located on a World Bank server in Washington, and relies on ITS to ensure adequate security over access to the Geneva server.

47. The ITS network administrator and his assistant are responsible for the administration of access rights to the network and e-mail systems but there is no documented computer security policy for UNCTAD that covers logical and physical access control procedures over its ICT systems, data and equipment.

48. A written security policy covering all aspects of IT security within UNCTAD should be drawn up. The policy would, *inter alia*, identify the persons who are assigned the most powerful access rights, both within and outside of UNCTAD, and can view or delete the documents and other data of others. These people should be identifiable and their rights and responsibilities should be clearly set out and approved by management.

49. ITS should take the lead in developing such a security policy and in setting standards that are in line with best practice.

Recommendation:

- UNCTAD, ITS should
  (a) Develop a security policy covering all aspects of IT security within UNCTAD. The policy should define the roles and responsibilities of staff associated with computer security, including non-UNCTAD staff. It should be supported by written procedures over the granting and modification of access rights and the removal of profiles in the case of terminated users;
  (b) Submit the security policy to the ICT Committee for review and approval;
  (c) Review and where necessary amend current access rights to

bring them in line with the security policy; and
(d) Perform a periodic (e.g. semi-annual) review of access rights to ensure they comply with the policy (Rec. 11).

Management response: *It is proposed to request UN/ICC to carry out a security policy assessment to be followed by the setting up of such policies. UN/ICC has already performed such work in the past (e.g. ITU).*
Implementation: As soon as possible

OIOS takes note of management's response. It will keep this recommendation open pending confirmation that the recommended actions have been implemented.

2. E-mail system

50. The United Nations International Computing Centre is providing UNCTAD's e-mail service. A person in the Centre and the Deputy Chief, ITS have administrator access rights.

51. OIOS did not perform a detailed assessment. However a brief review and discussions with management highlighted serious concerns on e-mail access security and the confidentiality of e-mails. One reason is that in the case of short-term staff members and consultants, ITS is not always aware of people who have terminated their contract and left UNCTAD. There may be instances where the e-mail account of a former staff member or consultant is still active, and can be accessed remotely via the Internet. When ITS is informed, access is normally removed one month after termination.

52. OIOS is recommending that management draws up a formal risk assessment arising from the current state of affairs and evaluate the cost of tightening control in this area against the risks involved. Certain measures, such as the alerting of ITS of leavers by Human Resources Management Section and the immediate disabling of the send function for terminated employees and consultants can be implemented at no cost to the organization.

Recommendations:

- Once set up, UNCTAD's ICT Committee should
  (a) Establish a policy over the granting and administering access rights to the e-mail system, including remote access, and the closure of e-mail accounts. This policy would form part of the overall security policy;
  (b) The send function should be disabled immediately upon termination and the read-only function retained for no longer than 30 days; and
  (c) Evaluate the option of e-mail encryption and tighter security over remote access (e.g. use of hand-held devices to generate random access codes) (Rec. 12).

Management response: *We believe that this issue should be included in the analysis we propose under recommendation # 11 above. E-mail accounts closure recommendations can be implemented*

once the information flow about staff movements is working smoothly (see recommendation #09).

OIOS takes note of management's response and agrees that the implementation of the recommended actions should be coordinated with that for recommendations 09 and 11. OIOS appreciates that developing and implementing policies is likely to take time, but in view of the risks involved with the systems as currently set up it urges management to assign priority to this area. It will keep this recommendation open pending confirmation that the recommended actions have been implemented.

E. Contingency and Business Continuity Planning

1. Contingency planning

53. The main computer equipment is housed in a room that is located directly above the Palette bar. There is no fireproof safe for the storage of back-up media anywhere within the UNCTAD premises.

54. Management should assess the risks arising from these circumstances and see whether a relocation of a computer room and/or the installation of a fire-proof safe for the storage of a complete set of back-ups is called for. OIOS also believes that UNCTAD should contact ITSD and obtain the latest Global IT physical security policies. These policies should be tailored and implemented for the entity.

Recommendation:

- UNCTAD, ITS should:
  (a) Assess the risk of the computer room's current location and the lack of a fire-proof safe and take appropriate action; and
  (b) Coordinate with the Information Technology Service Division to implement as soon as possible the Global IT physical security policies (Rec. 13).

Management response: *UNOG/ICTS is currently evaluating the design and designation of a new computer room which would be security proof and our proposal is to house UNCTAD's equipment in this facility once it is available. In the short term, we propose that an evaluation of the current risks associated with the location of our computer room be made part of the security analysis mentioned above, and decisions taken to minimize the risks based on this evaluation.*
Implementation: move to new computer room - to be coordinated with UNOG/ICTS; Risk assessment – ASAP.

OIOS takes note of management's response. In the wider context, OIOS would like to reiterate the recommendation to implement as soon as possible the Secretariat's Global IT physical security policies. This recommendation is kept open pending confirmation that the recommended actions have been implemented.

2. Business Continuity Planning

55. There are currently no formal plans which set out the procedures to be followed to ensure that in the event of a disaster affecting its computer facilities, UNCTAD would be able to mobilize alternate arrangements for processing data and continue to provide its core services efficiently while the facilities are being properly restored. While effective backup procedures and power supply protection provide a measure of insurance against system failures, in the event of a major disaster such as a fire, it is likely that the damage will not be restricted to the computer equipment but will also affect other areas.

56. Business continuity planning is wide in scope and requires input from all user departments. It requires coordination with external parties such as the suppliers of hardware, software and communications service and equipment.

57. The plan needs to be preceded by a risk assessment that will define the critical business functions and the systems supporting them, the different types of disasters, ranging from major malfunctions of equipment to large-scale disasters that would affect all the site activities. It would detail the key tasks and the individuals responsible for undertaking them, and the alternative arrangements to be made while the critical functions are being recovered.

58. The conduct of such an exercise is demanding on resources and OIOS suggests that UNCTAD takes advantage of the work that has already been undertaken by ITSD in the conduct of ICT Security Risk Assessments and Business Continuity Planning.

Recommendation:

- UNCTAD, ITS should:
  (a) Request the Information Technology Services Division at UN Headquarters to assist in carrying out an ICT Security Risk Assessment and seek to benefit from the work already undertaken by ITSD in relation to Business Continuity Planning; and
  (b) Draw up a project plan for the implementation of a Business Continuity Plan that details the stages to be followed to ensure that in the event of a major disaster, UNCTAD's critical operational functions are properly recovered and become operational within acceptable timescales. (Rec.14).

Management response: *This issue is also addressed by the ICT strategy paper, and a similar recommendation is made therein.*
Implementation: depends on ICT strategy endorsement.

OIOS takes note of management's response. It will keep this recommendation open pending confirmation that the recommended actions have been implemented.

V. FURTHER ACTIONS REQUIRED ON RECOMMENDATIONS

59. 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 already been recorded in the recommendations database. In order to record full implementation, the actions/documents described in the following table are required:

Recommendation No.	Additional actions and/or documents required from UNCTAD for closure of the open recommendations
AE2005/340/01/01*	Copy of the ICT Committee's Terms of Reference, approved by the SG, and minutes of the Committee's first meeting.
AE2005/340/01/02*	Copy of the vacancy announcement and the new Director for the Division of Management's terms of reference.
AE2005/340/01/03*	Copy of the ICT strategic plan for UNCTAD by its Secretary-General.
AE2005/340/01/04* AE2005/340/01/05*	Copy of the ICT Committee's Terms of Reference, approved by UNCTAD's SG, and minutes of the Committee's first meeting (recommendation 1), and a copy of the ICT strategy endorsed by UNCTAD's SG (recommendation 2).
AE2005/340/01/06	Document detailing the actions management will be taking to enhance time management and to determine the IT staff resources required to meet the ICT strategy objectives.
AE2005/340/01/07*	Copy of all the service level agreements.
AE2005/340/01/08*	Documentation setting out the policies and criteria for the replacement of all items of computer hardware and IT equipment within UNCTAD.
AE2005/340/01/09*	Written confirmation that systems for the effective management and control of computer hardware and software, and for maintaining an accurate list of user profiles are in place.
AE2005/340/01/10	Written confirmation that the recommended committee has been set-up and is functioning, and that an on-line system for users requests is operating.
AE2005/340/01/11*	Copy of the security policy approved by the ICT Committee and confirmation of completed review of access rights.
AE2005/340/01/12*	Copy of policy for granting and administering access rights to the e-mail system; written confirmation that the send function has been disabled immediately upon termination and the read-only function retained for no longer than 30 days; documentation supporting the evaluation of e-mail encryption security over remote access.
AE2005/340/01/13*	Copy of risk assessment evaluation of computer room location and actions to minimize risk; written confirmation that the Secretariat's Global IT physical security policies have been implemented.
AE2005/340/01/14*	Copy of the ICT Security Risk Assessment and Business Continuity Plan for UNCTAD.

* Critical recommendation

VI. ACKNOWLEDGEMENT

60. I wish to express my appreciation for the assistance and cooperation extended to the auditors by the staff of Information Technology Support.

Egbert C. Kaltenbach, Director
Internal Audit Division II
Office of Internal Oversight Services

ANNEX

Chief Information Officer responsibilities

The responsibilities of a Chief Information Officer within UNCTAD could include the following:

- Keep the organization's information management strategy and IT in alignment with its overall management strategy and priorities;
- Ensure that the information management policies and standards are strictly followed and the ICT infrastructure is well managed;
- Monitor compliance with the UNCTAD's ICT strategy and the global ICT policies of the Secretariat, including those over any new ICT initiatives;
- Ensure that accurate and timely information for decision-making is available to UNCTAD's senior executives;
- Establish security policies and procedures over access rights to the network, e-mail and application systems, as well as physical access to computer and communications equipment;
- Coordinate the purchase and allocation of hardware and other IT equipment;
- Establish procedures over the back-up and recovery of systems and data; and
- Coordinate business continuity planning.