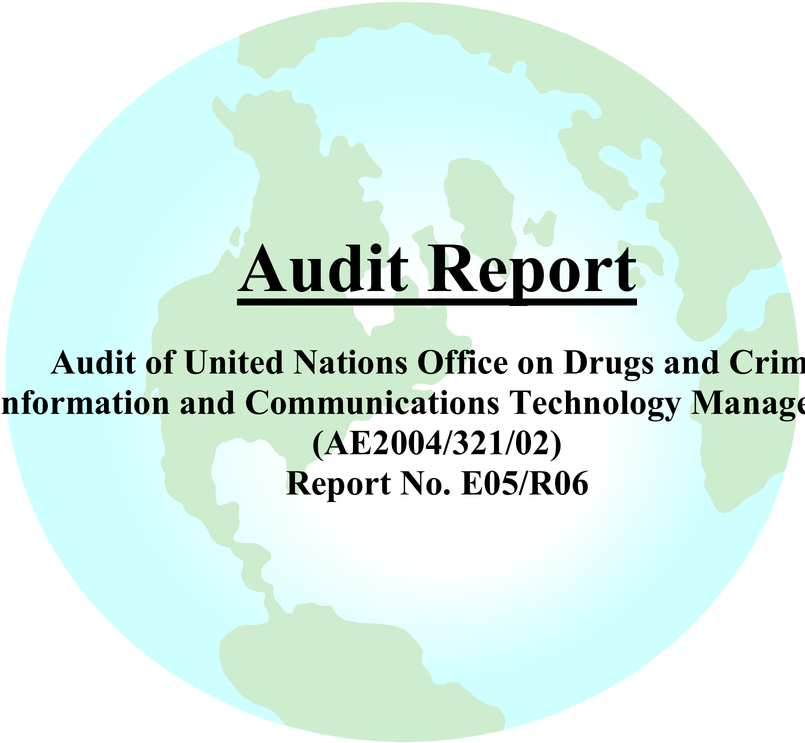
United Nations
Office of Internal Oversight Services
Internal Audit Division II



Audit Report

Audit of United Nations Office on Drugs and Crime Information and Communications Technology Management (AE2004/321/02) Report No. E05/R06

□ **Report date: 4 May 2005**

□ **Auditors:**

□ Mr. Leonard Gauci, Auditor-in-Charge

□ Mr. Esa Pääkkönen, Associate Auditor

UNITED NATIONS **NATIONS UNIES**

Office of Internal Oversight Services
Internal Audit Division II

OIOS audit of the United Nations Office on Drugs and Crime Information and Communications Technology Management (AE2004/321/02)

EXECUTIVE SUMMARY

Between 29 November and 6 December 2004, OIOS conducted an audit of UNODC's Information and Communications Technology Management function at its Headquarters in Vienna. *UNODC has accepted most of the recommendations and has initiated their implementation.*

OIOS assessed that, Information Technology Service (ITS) is making efficient use of the resources at its disposal to provide services to UNODC staff and other users of its systems. A number of areas at the management level need to be formalized to bring them in line with the policies of the Secretariat and best practices.

A governance structure covering all aspects of ICT within UNODC needs to be established. As a first step, UNODC should set up its ICT Committee in line with the requirements of ST/SGB/2003/17. This Committee would then oversee all major decisions regarding new software applications, define system and data ownership and monitor IT-related matters. *OIOS is pleased to note that management has accepted its recommendation in this regard and plans to have an ICT Committee operating by June 2005.*

UNODC requires a formal ICT strategy that is approved by the ICT Committee and the Executive Director. The strategy, which would be updated on an annual basis, should support the business plan of the Office and be aligned with the global ICT strategy of the Secretariat. *Management feels that the budget and project documents that are prepared and submitted for the review of various parties suffice and that an additional document is not required.* OIOS sees a distinction between budget/project planning and strategic planning and remains of the opinion that an ICT strategy document is required; both to comply with the provisions of ST/SGB/2003/17, and in particular, as a critical tool for UNODC's executive management to plan and monitor ICT-related matters.

In line with the ICT strategy of the Secretariat, proposals for new application systems, where feasible, should be backed by quantifiable returns on the investment made. The ICT Committee should establish a cost level above which proposals for new systems will need to be backed by an evaluation between in-house system development, subcontracting and the purchase of a packaged system. It should also establish criteria for delivery and user acceptance of such systems.

The situation regarding ITS resources in the areas of IMIS support and systems development calls for a study on capacity building. The feasibility of outsourcing within the UN organization should also be given consideration. UNODC should undertake a study to establish the optimum number of personnel and mix of skills required by ITS to deliver its services.   *Management has not accepted these recommendations, commenting that the Organization's policy of zero-growth budgeting would make any conclusions difficult to implement in practice.* OIOS is still of the opinion that an exercise on capacity building based on the ICT strategy should be used as an input to the budgetary process. In its comments to management's response OIOS also refers to various examples of outsourcing within the Organization. This option should not be dismissed outright but given consideration whenever the possibility arises (e.g. systems development). Accordingly OIOS is reiterating the recommendations made in this regard.

OIOS would like to see ITS taking a lead role in ICT matters concerning field offices with the objective of avoiding duplication, achieving streamlining and ensuring a standard that is at a similar level as the one in Vienna.

OIOS noted problems with regard to the accuracy of data received from UNDP's Atlas system for integration within UNODC's financial system (ProFi) and is recommending a study to look at options that would give the Office independence from the systems of third parties for its data.

OIOS is pleased to note that the services provided by ITS are articulated in service delivery agreements and is recommending that where applicable, these agreements incorporate specific provisions regarding core applications such as IMIS, ProFi, the National Drug Control System and the International Drug Control System as applicable.

UNODC should see that the work being done at United Nations Headquarters on ICT security and business continuity planning is extended to cover its core applications and ICT environment.

In the attached report, OIOS also makes several recommendations in the areas of ITS staff training, technical documentation, communication services, physical security and controls over access to databases. With the exception of a recommendation calling for a policy document on physical security, and which OIOS is reiterating, these recommendations have been accepted by management and have been, or are in the process of being implemented.

- May 2005 -

TABLE OF CONTENTS

I. INTRODUCTION

1. During November and December 2004, OIOS conducted an audit of the Information and Communications Technology management function within the United Nations Office on Drugs and Crime in Vienna. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

2. The present organizational structure of UNODC is regulated by ST/SGB/2004/6 of 15 March 2004 entitled “Organization of the United Nations Office on Drugs and Crime”, in conjunction with the Secretary-General’s bulletin ST/SGB/1997/5, entitled “Organization of the Secretariat of the United Nations” and ST/SGB/2004/5, entitled “Organization of the United Nations Office at Vienna”.

3. Information Technology Service (ITS) is one of three services that make up the Division for Management (the other two being the Financial Resources Management Service and the Human Resources Management Service). One of the core functions of the Division is that of providing information technology and substantive information management services for the United Nations Secretariat entities in Vienna and for the field offices of UNODC. This function is undertaken by ITS. The current organization chart for ITS is annexed to this report.

4. The findings and recommendations contained in this report have been discussed during the Exit Conference held on 6 December 2004 with the Director, Division for Management, the Chief, Financial Resources Management Service and Audit Focal Point, and the Chief, Information Technology Service. A draft of this report was communicated to the Director, Division for Management and the Audit Focal Point on 26 January 2005. Comments received on 8 March 2005 and subsequent clarifications by the Chief, Information Technology Service received on 22 April 2005 are reflected in the report in italics.

II. AUDIT OBJECTIVES

5. The main objectives of the audit were to evaluate the adequacy and effectiveness of controls and procedures to ensure:

- Proper governance over ICT, a well-defined ICT strategy backed by adequate budgeting and funding, and an appropriate ICT organizational structure and resources;

- The use of appropriate systems architecture, technology and application systems, appropriate procedures over the selection, development and implementation of systems and change control procedures;

- Efficient data capture and the integrity of data that is received from other core UN systems;

- The operation of computer systems and the provision of technical support to ensure a continued and efficient service to users;

- Security over systems and data;

- Support to users; and
- Business continuity planning.

III. AUDIT SCOPE AND METHODOLOGY

6. The review focused on the relevant areas of Information Technology controls that fall under UNODC. 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 UNODC (organization, systems and key performance indicators) through the completion of a questionnaire and an on-site visit during which the Auditor-in-Charge met with the Chief, Information Technology Service, the Chief, Financial Resources Management Service, and the Director, Division for Management, to explain the audit objectives, gather relevant information and listen to management's concerns. An audit programme covering all the audit objectives was developed on the basis of the above and executed during a site visit from 29 November to 6 December 2004. During this field visit, the audit team held interviews with staff, analysed applicable data and reviewed the available documents and other relevant records.

IV. AUDIT FINDINGS AND RECOMMENDATIONS

A. Establishing a governance structure for ICT

8. UNODC forms part of the Secretariat of the United Nations and is therefore governed by the Secretary-General's bulletin "Information and Communications Technology Board" (ST/SGB/2003/17).

9. The mandate of this Board is "to ensure a coherent and coordinated global usage of information and communications technology across departments and duty stations, in line with the objectives of the Secretariat and the central policy direction provided by the Steering Committee on Reform and Management" (ST/SGB/2003/17 paragraph 1.1). It calls for all departments and offices away from Headquarters to establish ICT committees and calls upon departments to establish departmental strategies aligned with the overall objectives of the Secretariat (ST/SGB/2003/17 of 21 November 2003, Section 4, paragraph 4.4).

10. UNODC does not have an ICT committee or other formal body to govern ICT in line with these requirements. An in-house system (Database of Databases) indicates data owners but use of this facility was not being applied consistently in this regard. OIOS also noted that ST/SGB/2004/6 of 15 March 2004 entitled "Organization of the United Nations Office on Drugs and Crime" does not specifically mention ITS and only gives a brief and generic description of the information and technology services to be provided (ST/SGB/2004/6 paragraph 8.2(e)).

11. There should be a well-defined governance structure for ICT that clearly identifies the parties and their responsibilities with regard to systems and data. An essential feature of the governance framework is clearly-defined ownership for all the systems that have been

implemented and the respective data. The governance function would be better supported if the core functions of ITS are defined.

Recommendation:

- UNODC should take steps to:
  (a) Set up its Information and Communications Technology Committee in line with Section 4.4 of ST/SGB/2003/17; and
  (b) Document the core functions of the Information Technology Service and present them to the ICT Committee for approval (Rec. 01).

Management response: *Accepted. Implementation: 1 June 2005.*

OIOS takes note of management's response. It will keep this recommendation open pending the receipt of the ICT Committee's Terms of Reference and minutes of the first meeting, and a copy of a document approved by the ICT Committee detailing the core functions of ITS.

- UNODC, ITS should ensure that ownership of systems and data be clearly evidenced and reflected in the Database of Databases (Rec. 02).

Management response: *Accepted. Implementation: 1 April and 1 October 2005.*
The Database of Databases has been in place and contains the needed fields for several years. In the majority of cases these fields are well-populated. However, the suggested review and tightening of these fields is welcomed. Semi-annual reviews are proposed.

OIOS agrees with management's proposed timing for the reviews. It will close this recommendation when it receives written confirmation that the reviews are taking place.

B. Implementation of a comprehensive ICT strategy

12. UNODC does not have an information and communications technology strategy that is approved at the highest level of the Office. The absence of a long-term strategy for ICT makes it difficult to identify and plan for acquisition of resources. This process may be initiated relatively late, and could result in delays in implementing systems.

13. The constant and rapid developments in ICT technology make it impractical to develop and implement a rigid ICT strategy but it should be possible to develop a strategy covering the next two biennia. This would be subject to periodic review, taking into account technological developments and any changes in the mandate of the Office.

14. OIOS has taken note of the presentation given by the Chief of ITS describing ITS policies (e.g. no outsourcing, integration), the work performed by the various units of ITS and other work that is in hand or planned for the near future. This would be a good basis on which to develop an ICT strategy that supports the mandate of the Office and is aligned with the ICT strategy of the Secretariat.

Recommendation:

- ➢ The future UNODC ICT Committee (Rec. 01) should request ITS to submit for its approval a rolling strategic plan for UNODC's IT services and applications covering the next two biennia. This plan should support the mandate and policies of the Office, include details of deliverables, timing and resource requirements, and be aligned with the global ICT strategy of the Secretariat. The ICT strategic plan should be endorsed by the Executive Director of UNODC (Rec. 03).

Management response: *Rejected.*
UNODC, ITS does not feel that another document is required as ITS, on a one, two and three year basis, prepares budget documents and project documents which include this information. These documents are passed through the formal review process of UNOV, UNODC, New York (Budget, ACABQ, and Fifth Committee), the Commission on Narcotic Drugs (CND), the International Narcotics Control Board (INCB), regular NDS User Group Meeting, etc. This extensive review and documentation process is felt to be sufficient, noting in particular that any activities which are not part of the budgetary approval process cannot in any case be implemented whether or not they are approved by any central body. Furthermore, ITS notes that we indeed (a) Follow A/57/620 (strategy document for us), (b) Provide input to A/59/265 (reporting on progress on the strategy) and (c) Are very active players in the ICTB (implementation planning and action re the strategy). These extensive strategy activities feed into our budget planning which controls our local within-context actions. This is also part of the budgetary process, in particular the alignment with the ICT strategy of the Secretariat and also in view of the newly formed Strategic Planning Unit of UNODC. Indeed ITS has no quarrel with the ICT strategy and notes that a high-level role is carried out by ITSD and the ICTB via extensive informal consultation, formal monthly videoconferences and a formal annual meeting (from which this document is written).

OIOS takes note of and appreciates the close involvement of ITS in the documentation process as outlined in the above response but sees a distinction between budget planning and strategic planning, and similarly, between project planning and ICT strategic planning. Furthermore, in addition to complying with the provisions of ST/SGB/2003/17, which calls for all departments and offices away from Headquarters to "… establish departmental strategies aligned with the overall objectives of the Secretariat" (para. 4.4), OIOS considers an ICT strategy document an essential tool for UNODC's executive management for planning and monitoring purposes. Accordingly OIOS reiterates its recommendation.

C. ITS organizational structure and staff resources

(a) Organization and resources

15. As a result of the March 2004 Secretary-General's bulletins on the organization of the Offices, the ICT function, which for the previous two years had been positioned within UNOV, moved back to UNODC. This repositioning reflects the fact that the majority of substantive operations fall under the mandate of UNODC.

16. The organizational structure for ITS looks rational and practical. The IMIS Technical Team however, only has two regular budget posts. The ratio of IMIS technical staff to users is 1:23 while for UNOG and ECA it is 1:57 and 1:46 respectively. IMIS is at the core of UNODC's IT Services and we understand that UNODC is likely to be requested to

implement upgrades to the Payroll and HR modules during 2005. This will put additional pressure on the existing resources.

17. Staff resources within the other ITS teams appear to be adequate to cope with day-to-day requirements but are thinly spread so any loss could, at least in the short-term, slow down operations considerably. OIOS noted the following areas where current staff resources are just adequate to cope with demand:

(a) PROFI Technical Team:
At the time of our audit, the post of Project Coordinator was still vacant while that of Project Manager, which is the only post funded from the regular budget, was on-loan from the Office of the Chief. The Project Manager felt that a second person was required for Warehouse Reporting.

(b) National Drug Control System (NDS)
Management felt that resources were limited for meeting deadlines and another person was required as back-up and for the team to follow-up matters at the user level.

(c) International Drug Control System (IDS)
The development of the systems had originally been outsourced to a company that was to allocate 12 people for a one-year period, but the contract was cancelled in September 2004 after users rejected the product and it was decided to develop it in-house. At the time of our visit to UNODC, there was only one person allocated to this area resulting in a lack of segregation of duties in the system design, programme and test functions. A developer and a programmer have since been allocated to support the System Manager and another programmer is being recruited.

18. In the case of applications development, the pace and quality depends on available resources. Apart from system design and programming, a software development project involves other processes such as testing, documentation, data migration and user training. If, as appears in the case with IDS, ITS is allocated insufficient resources and put under pressure to deliver systems within tight timeframes, the software that is delivered may not be of the best quality and contain an unacceptable number of errors. All this would ultimately result in additional costs and reflect badly on ITS, or, in the case of systems such as NDS and IDS that are used by external parties, on UNODC itself. ITS may also be constrained to turn down requests for system development due to unavailable resources. In this area, staff may only be required for the duration of the project and OIOS is of the opinion that management should explore the feasibility of engaging temporary staff, for example through the UN International Computing Centre. It may also be easier to obtain funds that can be utilized for this purpose instead of requesting additional posts.

Recommendation:

➢ UNODC, ITS should:
(a) Draw up a plan for capacity building based on an ICT strategy that is linked to the goals of the Office and to quantifiable returns on investment; and
(b) Assess the feasibility of outsourcing within the UN organization, in particular for skills related to system development and implementation (Rec. 04).

Management response: *Rejected.*
Re (a): Capacity cannot be built without a budget, and all such matters are carried out in the multitude of budgetary (RB, Support Budget, Core Budget, Drugs Fund, Crime Fund, Project, Workstation Support Programme, etc.) documents already produced annually. All such documents are heavily reviewed and scrutinized. While ITS appreciates the pureness of the Auditors comments in this regard, the reality of zero-growth budgeting means that the budgetary process defines the local implementation within the context of the overall strategy.
Re (b) ITS has followed the outsourcing environment for many years and continues to note the cost and effectiveness of outsourcing both within and outside the UN. ITS is disinclined to go down this path again.

OIOS notes that the report of the Secretary-General to the General Assembly titled "Information and communication technology strategy" deals with capacity building and the role of the ICTB and ICT committees in this regard. (A/57/620 paras. 75-80). It sees capacity building, linked to the ICT strategic plan, as an input by ITS to the budgetary process. Accordingly, OIOS reiterates its recommendation.

With regard to Rec. 04(b), A/57/620 para. 79 states that "In addition to building internal skills, selective outsourcing, especially for skills which tend to be commoditized and do not require institutional knowledge, will continue to be used." The report of the Secretary-General titled "Outsourcing practices" of 11 August 2004 (A/59/227) includes a number of activities in the field of ICT outsourced during the years 2002 and 2003. OIOS remains of the opinion that ITS should not dismiss the option of outsourcing within the Organization outright but only reach a decision after assessing its feasibility vis-à-vis utilizing in-house resources. OIOS is reiterating this recommendation for management's attention.

(b) Staff Training

19. ITS policy is that staff members should attend two training courses each year. Due to budgetary restrictions, however, the majority of staff are only receiving one training course. In the case of the Core Services Unit, not all staff members had the opportunity to attend a course during 2004. OIOS also noted that the training of ITS staff is not coordinated with Human Resources Management Service.

20. ITS staff are working in specialized areas that are subject to frequent technological developments and they require continuing training to keep up with these developments and provide the best service to users.

Recommendation:

- UNODC, ITS should make a detailed case for acquiring more training funds for its staff and liaise with UNODC Human Resources Management Service to optimize training opportunities and facilities (Rec. 05).

Management response: *Accepted. Implementation: 1 September 2005.*
UNODC's Human Resources Management Service (HRMS) has released additional funds for IT training in the 2004-2005 biennium and a permanent expanded framework is being built. The proposed recruitment of an IT training coordinator effective 1 May 2005 will enable this

recommendation to be actioned by the indicated date.

OIOS takes note of management's response. It will close this recommendation upon receipt of documentation supporting the new framework for IT training.

D. Selection, development and implementation of systems

(a) General

21. 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).

22. The Secretary-General's bulletin "Information and Communications Technology Board" established a 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 would review proposed ICT projects to see that the rationale behind the investment is justified, ensure that the total cost of projects is accurately projected, standard development methodologies are applied and all relevant documentation is available.

23. UNODC's current policy is not to buy off-the shelf packages and there is no evaluation between in-house development and ERP solutions. Furthermore, as indicated in paragraph 10, UNODC's ICT Committee has not yet been established. Until this committee is established, the Office will not have a role in the PRC.

24. The total cost of developing and implementing a system and the source of funding should be determined before the system is commissioned and there should also be an evaluation between systems development and an ERP solution. In the case of ProFi, $4 million had been invested in implementing the system by the end of 2002. OIOS is not aware of any comparative analysis between the costs and benefits of hiring consultants to develop ProFi and other options such modifying IMIS. The Board of Auditors questioned the reasons behind the decision to implement ProFi (BOA Management Letter dated 26 March 2002) rather than an IMIS-based tool. The problems left behind by the consultants were resolved after significant allocation of in-house resources. A more thorough evaluation prior to selection could have avoided these problems.

25. There should also be clear criteria, together with formal user acceptance, to define the point when a project is complete and the user department takes over as system owner. Such criteria have been absent and OIOS noted that user approval of new application systems, for example in the case of NDS and web-site development, is not always evidenced.

Recommendation:

- UNODC should ensure that:

(a) The ICT Committee establishes a cost level above which proposals for new systems will need to be supported by an evaluation that includes a financial impact and a comparative analysis of purchasing a package system against developing it in-house, or subcontracting it. Such proposals, where feasible, should be backed by quantifiable returns on the investment made; and
(b) The scope of a software development project is defined at the outset and the criteria for systems delivery and acceptance are incorporated in software development agreements with the users (Rec. 06).

Recommendation 6(a) has been redrafted and is awaiting response from management.

Management response: *Recommendation (b) is accepted and has been completed. A change in management has taken place which has immediately lead to this very desirable result.*

OIOS takes note of management's response. It will keep this recommendation open pending receipt of the policy on systems selection and documentation supporting the implementation of Rec. 06(b).

(b) Technical documentation

26. OIOS noted some inconsistencies in the Database of Databases, which is the tool used to record information about UNODC's application systems. The indicated status of the application/database was not always consistent with the actual project status – for example the status would be marked as "inactive" when its project status might be "production". The Database of Databases is an important management tool and the information should be kept up-to-date.

27. The UNODC Web Management Team, which is made up of two staff members, has done a lot of useful work in developing new websites and redesigning existing ones. However, OIOS noted that requests for web-site development are not documented and technical documentation is not complete. This would create problems with continuity if the current staff members were no longer available.

<u>Recommendation:</u>

- ➢ UNODC, ITS should:
  (a) Carry out periodic reviews to check that the information in the Database of Databases is consistent with the actual status of projects; and
  (b) Ensure that all requests for website development are documented and that technical documentation supporting all websites is available (Rec. 07).

Management response: *Accepted. In the case of (a), reviews will be carried out on 1 April and 1 October 2005; (b) has been completed.*
It should be noted that all websites supported by ITS run on the same technical environment

and use the same Content Management System (date of documents 26 March 2004 and October 2004; new document will be completed 14 March in time for the next round of training).

OIOS takes note of management's response. It will close this recommendation when it receives written confirmation that the review envisaged for April has been completed.

(c) Software installation licences

28. For internal control purposes and to comply with statutory requirements it is important for ITS to have a complete and accurate list of all software installation licences.

29. Software installation licences for the individual workstations in the Vienna offices are tracked through the ZenWorks database. This database combines the installation base information with purchase details recorded in IMIS. Any discrepancies are reported to the relevant unit and a purchase of the missing licences is requested. The OiC of the Core Services Unit prepares the discrepancy reports. This is a manual procedure that is time-consuming and difficult to maintain since ITS is not automatically notified of licence purchases. Licences for workstations in the field are not handled by ITS in Vienna but by the Global Field Office Support team in India.

30. The situation will become more complicated if ITS takes on a more direct role in supporting field offices. For example procedures will be required for managing different terms when dealing with licences that are on a global rather than local basis and where users who are on mission and have access to their own data install software for use on a PC that belongs to the field office.

Recommendation:

- UNODC, ITS should seek to implement a system whereby the Core Services Unit is immediately informed of the purchase of new software installation licences and implement a policy over these licenses that covers all of UNODC's operations (Rec. 08).

Management response: *Accepted. Implementation: 1 July 2005.*
For Vienna, ITS is now using Novell ZENWorks to poll all workstations and determine the licensing situation. This is a truly quantitative method as it finds the true situation on the ground and does not rely on reports from any person. Action is being taken to remedy any current discrepancies. An application is currently being developed for the Field Offices that allows recording of all licenses.

OIOS takes note of management's response. It will keep this recommendation open pending the receipt of documentation showing that the system for recording all software installation licenses is functioning.

E. Information management at the field office level

31. ITS is focusing on providing Global Services to all UNODC field offices. The purchasing of hardware is centrally controlled through the office in India. ITS is involved in planning

and budgeting for ICT resources as far as ITS activities at headquarters are concerned but not for IT resources in the field offices. ITS does not monitor purchases made through the India office, and does not have a say in the systems that are developed or purchased at the field office level. Neither is there monitoring of such activity.

32. Apart from the core systems such as IMIS and ProFi, there could be various applications in the field offices covering work related to the operations or administrative work of that office. Past experience within the UN system shows instances where the absence of central monitoring led to a proliferation of applications and databases, often with duplication of data, and a lot of time and effort was subsequently required to achieve streamlining.

33. To avoid the risk of duplicate data entry and data storage, OIOS is of the opinion that development of software applications and databases above a certain level should be centrally monitored to ensure that this is done on a cost-benefit justification and there is no duplication or incompatibility. These projects would be tracked through the Database of Databases.

34. OIOS takes note of the significant efforts made by ITS over the past 12 months to bring the level of service provided to field offices on a par with that received by users in Vienna. It is also of the opinion that ITS should take a more active role with field offices as coordinator of the Office's IT strategy and policies. This could take the form of guidelines and briefings on matters such as the IT Strategy, the creation of the ICT Committee and other aspects of ST/SGB/2003/17, the ICT Strategy of UNODC and the Secretariat's policy on the use of ICT resources and data (ST/SGB/2004/15).

Recommendation:

- ➢ Once set up, UNODC's ICT Committee should establish guidelines, policies and standards for ICT projects at the field office level and set a ceiling for ICT field projects with the stipulation that all new proposals from the field to acquire or develop application systems and databases that exceed such ceiling should be subject to review and approval by the Committee. Approved projects should be recorded and tracked through the ITS Database of Databases (Rec. 09).

Management response: *It is very difficult for HQ to decide on appropriate field office projects and it is also inappropriate for HQ to delay advances in the field. This is why ITS has a team in the field (in particular in India, Uzbekistan and Mexico) tasked with this responsibility. The feedback from UNODC Field Representatives and included in HRMS and FRMS mission reports has been positive in the extreme. While ITS continues to have reservations with respect to the appropriateness of the Committee vis-à-vis field office systems, it can indeed accept this recommendation based on the cost level recommended by OIOS above.*

OIOS takes note of management's response. It will keep this recommendation open pending receipt of a copy of the guidelines, policies and standards set by the ICT Committee for ICT projects at the field office level that exceed the set cost level.

- ➢ UNODC, ITS should supplement its main ICT strategy with a plan detailing its support to field offices and measures to ensure that guidelines, policies and standards established at

UNODC headquarters are consistently applied in the field (Rec. 10).

Management response: *Accepted. Implementation: 30 November 2005.*

OIOS takes note of management's response. It will keep this recommendation open pending receipt of the plan detailing the support of ITS to field offices.

F. Data capture and interfaces with other UN systems

35. ITS is responsible to address the interfacing between UNODC's systems and data with other systems used by the Organization such as IMIS and Galaxy. As such, it should have proper mechanisms in place to ensure the completeness and integrity of all data that is uploaded into UNODC's systems from other systems, and that no corruption of UNODC core data results from such uploads.

36. Due to staff limitations, UNDP has been engaged to make disbursements on behalf of UNODC's field offices and provide certification and approval services for bank transactions. Transactions are recorded in UNDP's Atlas system. For the field offices to monitor what UNDP has expended on their behalf, data from Atlas has to be integrated into UNODC's financial system (ProFi). Our brief discussions and a review of e-mail exchanges between UNODC and UNDP finance personnel indicate that the accuracy of the data received from Atlas is questionable. Indications point to a user problem, perhaps due to inadequate training. Nevertheless, this issue it is taking up considerable time for both ITS and finance staff to resolve and impacts on the timeliness of UNODC's financial records.

37. Whether UNODC should seek to move away from UNDP and the Atlas system and to what extent this would be feasible is beyond the scope of this audit. However, given the amount of potential monetary and time savings, the reduced risk of error and quicker turnaround time regarding the availability of financial reports, a detailed study of this option is called for.

Recommendation:

- ➢ UNODC, FRMS with the support of UNODC, ITS should undertake a study to determine the feasibility of, and the potential savings from adopting an alternative system to Atlas for use by UNODC field offices (Rec. 11).

Management response: *Accepted.*
A new IT system has been developed by FRMS and ITS and is, as of January 2005, under pilot in Uzbekistan. Potential savings are fully documented by FRMS. FRMS has in place a plan for broad deployment following completion of this pilot.

OIOS takes note of management's response. It will keep this recommendation open pending the receipt of documentation showing potential savings and the deployment plan.

G. Technical and network support

38. In the Vienna International Centre there are two telephone switches (PBXs). One of these is used by the International Atomic Energy Agency. The second PBX is used by the other

organizations. The VIC's Building Management Service technically controls this PBX but UNODC is responsible for operating the communications. The current arrangement could be rationalized so one organization would have responsibility over the whole process.

39. The ITS Communications and Infrastructure Team has staff dealing with the switchboard and fax/videoconferencing systems. Technical operations are currently dealt with by UNIDO. This arrangement may be restructured to merge the switchboard and technical operations.

Recommendation:

➢ UNODC, ITS should:
(a) Seek ways to improve the efficiency of communications technology service between the UN organizations in the Vienna International Centre through a reorganization of the PBXs; and
(b) Liaise with UNIDO to evaluate a restructuring of the communications function (Rec. 12).

Management response: *Accepted. Implementation: 1 April 2006.*
Please note that the outcome of this initiative is uncertain.

OIOS takes note of management's response and appreciates that the outcome the initiative depends on third parties. It will keep the recommendation open pending the receipt of documentation supporting the review and evaluation of the communication function within VIC.

H. Logical access controls

40. Our review showed that access rights to Lotus Notes databases were not handled in a consistent manner and sufficiently restricted. Database security was set at the "Default" access. This access level enables any user to access all the information held in the database. Examples noted during the audit:

- Two Lotus Notes databases containing personnel information. (One of these databases contains sensitive information about staff members and their dependants including grade, birth date, nationality and information on dependants and any disability).
- The staff data consistency database (comparing Lotus Notes, IMIS and the Central Registry), where the default user had design rights.

41. Our review was not an in-depth one and unrestricted access to other databases containing sensitive or non-public information may be available.

Recommendation:

> UNODC, ITS should request data owners to define access rights of their applications and their data and to perform a periodic (e.g. semi-annual) review of access rights to ensure they comply with the defined policy (Rec. 13).

Management response: *ITS will ensure that the data owners review access rights immediately. A semi-annual review by data owners is a very good recommendation and such a review will be carried out on 1 April and 1 October of each year.*

OIOS takes note of management's response. It will keep this recommendation open pending written confirmation that the first periodic review has been completed.

I. Physical security

42. The main computer equipment is housed in five locations, all within the Vienna International Centre. Work at the various locations is subject to the asbestos-cleaning programme currently being undertaken within the Centre.

43. OIOS noted that the container housing back-up and other equipment is accessed via a normal lock and is sited at ground level. The four windows of the computer room and another two in the adjoining operator room are not adequately protected from unauthorized access and security cameras to monitor the area were not yet functional. Electricity and network cabling on the outside is exposed and vulnerable to wilful damage.

44. Physical security measures over computer installations and equipment within UNODC are the responsibility of Safety and Security Service. The Chief, ITS said that there was on-going coordination between ITS and SSS but he was not aware of documented policies and procedures over physical security. ITS planned to follow the Global IT physical security policies that are currently being developed at UNHQ.

Recommendation:

- UNODC, ITS should:
  (a) Coordinate with the Safety and Security Service to develop a security policy supported by procedures for computer installations and equipment;
  (b) Take steps to strengthen the security over access to the container housing back-up and other equipment by implementing more secure locking facilities, window grids, and camera surveillance. Steps should also be taken to provide protection over the external cabling; and
  (c) Coordinate with UNHQ to implement as soon as possible the Global IT physical security policies that are currently being developed in New York (Rec. 14).

Management response: *Recommendation (a) is rejected. Given the continuing price reduction in IT equipment and the essentially zero theft and maltreatment levels, it is difficult to see that any substantial improvement over the current system could be made. Recommendations (b) and (c) are accepted. In the case of the former, work is already in progress and is expected to be ready by 1 July 2005. ITS is implementing smart-card door access, motion detection and window breakage detection. The external cabling is protected against accidental damage by a three-phase power line of such a physical thickness and voltage as to deter errant activities. With regard to (c), full implementation is expected by 31 December 2006.*

Physical security of IT installations and equipment is an area where one will find some measure of overlap between two or more services. In the opinion of OIOS, an informal understanding between current personnel may be a workable arrangement but a policy document outlining the respective roles and responsibilities is required for reference and continuity. It is up to management to decide the detail of supporting procedures. OIOS is therefore reiterating recommendation 14(a) for consideration by management and will keep it open pending management's further reply.

OIOS takes note of management's response regarding (b) and (c) and will keep these recommendations open pending written confirmation that the corresponding measures have been fully implemented.

J. <u>ICT services and user support</u>

45. OIOS is pleased to note that the services provided by ITS within UNODC-UNOV and to United Nations Programme and Satellite Entities are documented in Service Level Agreements and Service Level Statements. The existing SLAs and SLSs are at the ITS level and do not refer to specific applications. OIOS feels that it would be good practice and of benefit to both ITS and users if the respective responsibilities, rights and obligations regarding core systems such as IMIS, ProFi, NDS and IDS are documented.

Recommendation:

- ITS should update the existing Service Level Agreements to include, as appropriate, specific reference to the respective responsibilities, rights and obligations regarding IMIS, ProFi, NDS and IDS. (Rec. 15).

Management response: *Accepted.*

OIOS takes note of management's response. It will keep this recommendation open pending receipt of the updated SLA's.

K. ICT Security and Business Continuity

46. There is a Business Continuity Plan that covers IMIS but UNODC does not have a documented security policy covering all its applications or a Plan aimed at ensuring that in the event of a disaster, UNODC will continue to provide its core services effectively while properly restoring the facilities. While ITS has disaster recovery plans for critical systems and has been trying to build redundancy into systems (as with the new ProFi servers), business continuity is a wider issue and requires cooperation and coordination with all departments.

47. In its report following a post-implementation review of IMIS, OIOS had recommended that Secretariat's Information Technology Services Division follow up on the Board of Auditors' recommendations for undertaking an information systems risk analysis and the implementation of an information systems security policy. At the end of September 2004, ITSD has completed four ICT Security Risk Assessments and planned to complete assessments for all OAHs by the end of 2004. These Security Risk Assessments do not yet cover UNODC.

48. In addition to completing the ICT Security and Business Continuity Policy review by the end of 2004, ITSD has initiated the preparation of an ISO17799 information security compliance project that will define and regulate procedures for system failures and disaster recovery within a comprehensive ICT security framework. Business Continuity will be addressed under this project. Proposals being formulated by ITSD for Global Business Continuity also recognize the significant business impact of the non-availability of IMIS.

49. ICT Security and Business Continuity call for careful and thorough planning, and require significant allocation of funds and staff. They also require coordination between several parties such as the suppliers of hardware, software and communications equipment.

Recommendation:

- ➢ UNODC, ITS should:
  (a) Request the Information Technology Services Division at UN Headquarters to include its systems in the ICT Security Risk Assessments; and
  (b) Actively participate and seek to benefit from the work already undertaken by ITSD in relation to Business Continuity Planning and ensure that the applications for which it is responsible are adequately covered in such plans (Rec. 16).

Management response: *Accepted and completed.*
NY has already carried out an ICT Security Risk Assessment. Their report has been submitted to UNODC and necessary action taken. ITS has taken part in all ITSD initiatives in this

regard, has attended the relevant meetings in NY, taken part in the relevant videoconferences, etc. The next meeting in this regard will take place in April in NY and ITS will attend. The first benefits to this relate to the upgrading of the UNPSN link to NY and the provision this year by ITSD of $135,000 to support the upgrading of ITS' Enterprise Data Centre (EDC).

OIOS takes note of management's response. It will close this recommendation once it receives a copy of the Security Risk Assessment and Business Continuity Plans.

V. FURTHER ACTIONS REQUIRED ON RECOMMENDATIONS

50. 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 UNODC for closure of the open recommendations**
AE2004/321/02/01*	Copy of the Terms of Reference and minutes of the ICT Committee's first meeting, and a document detailing the core functions of ITS.
AE2004/321/02/02*	Confirmation that reviews of the Database of Databases to check the accuracy of systems and data ownership are taking place.
AE2004/321/02/03*	Copy of the approved ICT strategic plan for UNODC.
AE2004/321/02/04*	Copy of UNODC's plan for capacity building supporting the ICT strategy and updated policy on outsourcing assessments.
AE2004/321/02/05*	Copy of documentation supporting the new framework for IT training.
AE2004/321/02/06*	Copy of the ICT Committee's policy on systems selection and an example of the updated software development agreements with users.
AE2004/321/02/07	Confirmation that the reviews of the Database of Databases to check that the information is consistent with the actual status of projects are taking place.
AE2004/321/02/08	Confirmation that the system for recording all software installation licenses is functioning.
AE2004/321/02/09*	Copy of guidelines, policies and standards set by the ICT Committee for ICT projects at the field office level which exceed a set cost level.
AE2004/321/02/10*	Copy of plan detailing the support of ITS to field offices.
AE2004/321/02/11*	Copy of FRMS documentation showing potential cost savings and deployment plan.
AE2004/321/02/12	Documentation supporting the review and evaluation of the communication function within VIC.
AE2004/321/02/13*	Confirmation of completed review of access rights to the Lotus Notes databases.
AE2004/321/02/14*	Copy of security policy and written confirmation that the measures related to Rec. 14 (b) and (c) have been fully implemented.
AE2004/321/02/15	Copy of updated Service Level Agreements.
AE2004/321/02/16*	Copy of the ICT Security Risk Assessment and Business Continuity Plans.

(* Critical Recommendations)

VI. ACKNOWLEDGEMENT

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

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