INTERNAL AUDIT DIVISION

AUDIT REPORT

Information and communications technology governance and security management at the International Criminal Tribunal for Rwanda

ICTR should implement additional controls for improving the delivery of services and the security of information and assets

25 April 2011
Assignment No. AT2010/260/01

United Nations Nations Unies

INTEROFFICE MEMORANDUM MEMORANDUM INTERIEUR

OFFICE OF INTERNAL OVERSIGHT SERVICES · BUREAU DES SERVICES DE CONTRÔLE INTERNE

INTERNAL AUDIT DIVISION · DIVISION DE L'AUDIT INTERNE

TO: Mr. Adama Dieng, Registrar
A: International Criminal Tribunal for Rwanda

DATE: 25 April 2011

REFERENCE: IAD: 11- 00372

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

SUBJECT: **Assignment No. AT2010/260/01 - Audit of information and communications technology**
OBJET: **governance and security management at the International Criminal Tribunal for Rwanda**

1. I am pleased to present the report on the above-mentioned audit.

2. Based on your comments, we are pleased to inform you that we will close recommendations 2, 4, 5, 6, 7, 11, 12, & 13 in the OIOS recommendations database as indicated in Annex 1. In order for us to close the remaining recommendations, we request that you provide us with the additional information as discussed in the text of the report and also summarized in Annex 1.

3. Please note that OIOS will report on the progress made to implement its recommendations, particularly those designated as high risk (i.e., recommendation 9 and 11) in its annual report to the General Assembly and semi-annual report to the Secretary-General.

cc: Mr. Choi Soon-hong, Assistant Secretary-General, Chief Information Technology Officer, OICT
Dr. Sarah Kilemi, Chief, Division of Administrative Support Services, ICTR
Mr. Swatantra Goolsarran, Executive Secretary, UN Board of Auditors
Mr. Rohan Wijeratne, Board of Auditors
Ms. Susanne Frueh, Executive Secretary, Joint Inspection Unit
Mr. Mario Baez, Chief, Policy and Oversight Coordination Service, Department of Management
Mr. Byung-Kun Min, Special Assistant to the USG-OIOS
Ms. Corazon Chavez, Chief Nairobi Audit Service, OIOS
Ms. Amy Wong, Programme Officer, Internal Audit Division, OIOS

INTERNAL AUDIT DIVISION

FUNCTION

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

CONTACT INFORMATION

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

DEPUTY DIRECTOR:
Gurpur Kumar: Tel: +1.212.963.5920, Fax: +1.212.963.3388,
e-mail: kumarg@un.org

EXECUTIVE SUMMARY

Information and communications technology governance and security management at the International Criminal Tribunal for Rwanda

The Office of Internal Oversight Services (OIOS) conducted an audit of information and communications technology (ICT) governance and security management at the International Criminal Tribunal for Rwanda (ICTR or the Tribunal). The overall objective of the audit was to assess the adequacy and effectiveness of internal controls over ICT governance and security management, and to determine compliance with applicable United Nations regulations, policies and procedures. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

ICTR had in place a dedicated section for managing its ICT infrastructure and for providing ICT support to the activities of the Tribunal. In particular, OIOS observed the following good practices:

(a) A working group for the development of a joint archiving strategy was created to collaborate on standardization and classification of the Tribunal's records;

(b) Strategies existed for rationalizing the use of equipment (i.e. shared printers, recycling of equipment parts). However, these were not documented in a formal policy;

(c) Standards and statements of good practice existed in some areas. However, this approach was not consistent across the Tribunal;

(d) The ICTR network was adequately segmented; and

(e) The Office of the Prosecutor (OTP) documented a "statement of standard terms and conditions for the electronic disclosure system (EDS)" which was signed by defence lawyers before they were given access to the system.

Although the Tribunal has implemented the good practices listed above, additional controls mechanisms and procedures are needed in the areas of ICT governance, service delivery and information security. These controls and procedures should include:

(a) Defining an ICT strategic planning process and an ICT governance framework;

(b) Improving information security management processes and establishing business continuity management procedures;

(c) Documenting and implementing procedures for ICT operations and resources including: (i) access and password management; (ii) network capacity management; and (iii) asset management;

(d) Deploying communication links and archiving procedures for the United Nations Detention Facility (UNDF); and

(e) Documenting and implementing standard procedures for data classification across the Tribunal.

TABLE OF CONTENTS

I. INTRODUCTION

1. The Office of Internal Oversight Services (OIOS) conducted an audit of information and communications technology (ICT) governance and security management at the International Criminal Tribunal for Rwanda (ICTR or the Tribunal). The audit reviewed the risks and controls related to ICT governance and security because they are critical to the operations of the Tribunal. The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing.

2. ICTR was established for the prosecution of persons responsible for genocide and other serious violations of international humanitarian law in the territory of Rwanda between 1 January 1994 and 31 December 1994. ICTR is governed by its Statute, which is annexed to the Security Council Resolution 955. By resolution 977 of 22 February 1995, the Security Council decided that the seat of the Tribunal would be located in Arusha, United Republic of Tanzania.

3. The Tribunal consists of three organs: The Chambers and the Appeals Chamber; The Office of the Prosecutor, in charge of investigations and prosecutions; and The Registry, responsible for providing overall judicial and administrative support to the Chambers and the Prosecutor.

4. The Security Council in its resolutions 1503 (2003) of 28 August 2003 and 1534 (2004) of 26 March 2004, called on the Tribunal to take all possible measures to complete investigations by the end of 2004, to complete all trial activities at first instance by the end of 2008, and to complete all work in 2010. However, the Tribunal in its completion strategy report (S/2010/259) stated that due to obstacles faced, it will not be in a position to complete all its work in 2010. In this regard, the Security Council in resolution 1932 (2010) extended the terms of office of all trial judges at the International Tribunal based on the Tribunal's projected trial schedule and the terms of office of all appeals judges until 31 December 2012.

5. The Information Technology Support Section (ITSS) of the Tribunal is composed of the Electronic Data Processing Unit (EDP) and the Communications Unit. ITSS is part of the Registry and is responsible for providing the Tribunal's ICT infrastructure and support to enable the achievement of the ICTR mandate.

6. ITSS supports a base of 1,000 users in Arusha. Additionally, it has a regional office in Kigali comprising of about 150 users with its own ICT support team.

7. For the biennium 2010-2011, the General Assembly approved initial appropriations for ICTR of $227,246,500, and authorized 693 posts for 2010 and 628 posts for 2011. The projected 2010-2011 appropriation for ITSS is $2,951,200.

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

II. AUDIT OBJECTIVES

9. The main objectives of the audit were to assess the adequacy and effectiveness of controls established in ICTR for:

(a) Governing, managing and protecting ICT resources, assets and data;

(b) Defining and assigning ICT roles, responsibilities, and reporting lines;

(c) Supporting ICT strategic planning, monitoring, reporting, and continuous improvement; and

(d) ICT security management, risk assessment and vulnerability testing.

III. AUDIT SCOPE AND METHODOLOGY

10. The audit was conducted at ICTR in Arusha, Tanzania and covered the years 2009 and 2010. The OIOS review included: (a) Policies, standard operating procedures and guidelines; (b) Analysis of the information provided in response to the audit questionnaires submitted for governance and security; (c) Interviews with representatives and staff from substantive areas and the Tribunal support offices; (d) Vulnerability tests on selected critical hosts and scans of the Tribunal's network; (e) Application controls and security review of two critical applications (ZYLAB & TRIM); and (f) Visit to the United Nations Detention facility (UNDF).

IV. AUDIT FINDINGS AND RECOMMENDATIONS

A. Strategic planning and governance

11. A strategic plan should define and document how the ICT function will support the organization in achieving its objectives, ensuring alignment between strategic goals and ICT activities. ICTR had a strategy for the completion of its activities related to trials and the judicial process. However, this strategy did not include provisions explaining how the ICT function and services would contribute and support the Tribunal's core functions, processes and objectives. In addition, the completion strategy did not include an exit/liquidation strategy for the administrative support of the Tribunal and provided no direction and planning for transitioning the ICT infrastructure and services upon completion of the Tribunal's activities.

12. An ICT governance framework should define the criteria and procedures for directing and monitoring ICT investment, applications and infrastructure. ICTR did not have an ICT governance framework in place. Furthermore, there

was no dedicated ICT committee within the Tribunal to serve as a focal point for approving the goals and direction of the ICT function.

13. The lack of overall direction concerning the ICT infrastructure resulted in a fragmented approach to ICT service delivery within the Tribunal, since ICT services were also provided by two other units within the Court Management Service (CMS) and the Office of the Prosecution (OTP). In this regard, the following conditions were observed:

(a) Duplication of efforts, ineffective rationalization of staff, equipment and funding resources; and

(b) Operational isolation and ineffective coordination of ICT systems resulting in:

(i) The implementation of multiple applications/job functions providing and supporting the same activities (e.g. 3 helpdesks); and

(ii) Limited collaboration between the various stakeholders on ICT issues, and opportunities and capabilities not leveraged.

Recommendation 1

(1) ICTR should: (a) Document a formal ICT strategy to define how ICT services will contribute and support the Tribunal. The strategy should take into consideration the need to ensure continuous provision of ICT services and support until the completion of Tribunal's activities; and (b) Establish an ICT steering committee comprising representatives of the Tribunal's major stakeholders.

14. *ICTR accepted recommendation 1 stating that it will constitute a local ICT Committee in accordance with the ICT governance framework established by the Office of Information and Communications Technology. The local 1CT Committee will assume responsibility for developing a formal ICT strategy covering the entire ICTR and high level plan for implementing the strategy.* Recommendation 1 remains open pending the documentation of a formal ICT strategy.

ICT budget

15. The costs and benefits associated with the Tribunal's ICT infrastructure should be visible, comparable and consistent and allow for ongoing review of the overall ICT budget and budgets specific to individual ICT programmes. The Tribunal did not have a system in place for classifying, monitoring and reporting on the costs associated with the provision of ICT services within the Tribunal. Costs associated with ICT operations within CMS and OTP were merged with other operational costs, even though the ICT operations within these areas were

clearly identifiable. OIOS also noted that ICTR faced funding limitations as a result of the scheduled completion of its operations. However, in the 2010-2011 budget submission there was an indication that requests for ICT service provision will increase instead of decrease as a result of the completion strategy. Despite this, ITSS faced reduction in posts and budget cuts and risked the ability to continue supporting and managing the ICT infrastructure effectively.

16. A human resources (HR) plan should enable the organization to manage its staffing requirements in line with its strategic programme. The Secretary-General in his report A/64/478 on the budget for the biennium 2010-2011 outlined the difficulty in retaining competent, knowledgeable and experienced staff for the Tribunal, which it can no longer offer long term job security. The Secretary-General also indicated that the continued service provided by staff in areas with heavy workloads was essential for ensuring timely completion of the trials and a smooth transition to the future residual mechanisms.

17. OIOS noted that ITSS did not document an HR plan for ensuring the continuity of its services in line with the completion strategy of the Tribunal's operations. ITSS was reliant on ICTR dedicated staffing resources and interns, and did not consider the use of additional resources from other United Nations Organizations such as the United Nations Volunteers (UNV) or the International Computing Centre (ICC). This condition exposes ITSS to risks of being unable to recruit and retain adequate human resources for providing support and services to the Tribunal. These risks were particular evident in the following cases:

(a) The help desk was understaffed and had 4 support staff for every 1000 users (1:250), while the industry best practice is 1:50;

(b) One system administrator supported all production servers and Lotus Notes applications (including email) used by 800 users + 100 interns without any backup; and

(c) One network administrator (2 out of 3 posts were vacant in this area) was responsible for both network operations and information security, thereby creating a conflict in roles and responsibilities, and over-reliance on a single individual for a critical function.

Recommendation 2

(2) ICTR should: (a) Review its budget structure and ensure transparency of all ICT associated costs across the Tribunal; (b) Document and periodically review its human resources plan and ICT staffing requirements, ensuring that they are aligned with the Tribunal's completion strategy; (c) Maximize existing ICT resources and undertake a rationalization exercise of existing ICT staffing resources and equipment within ITSS, the Office of the Prosecution and Court Management Services; and (d) Consider the use of the services provided by the International Computing Centre

and United Nations Volunteers to provide staffing resources in support of ICT service requirements.

18. *ICTR accepted recommendation 2 stating that it agreed that keeping the OTP Systems Support Unit supporting its specific applications is not ideal in terms of resources utilization, and a better use of existing expertise would result in less effort duplication and a better user experience. A discussion is already under way to achieve this objective in planning for ICT services for 2012-2013. However, it stated that for network administration, OTP and other organs of the tribunal each use a separate network domain, which it will be kept separated due to the independence of each organ and their specific ICT requirements. ICTR further stated that it agreed that services such as user account management, permissions assignment, LAN administration, etc. will be the kind of tasks that can typically be executed by either ICTR-IT or OTP-SDU staff, if such functions are centrally planned and administered with documented service level agreements with all organs. The local ICT Committee is envisaged to assume the responsibility for ensuring transparency of ICT associated costs across the Tribunal. ICTR also stated that it currently has several legacy projects underway in the OTP and in the Registry. Since these projects require additional ICT support, it is expected that ICTR resources will witness an increase in the short term as it prepares for handover of information to the Residual Mechanism (RM). This initial investment in preparation will assist the RM in maintaining a lean and efficient staff component. Integration of staff from JRAU and OTP in the upcoming planning period should also reduce the detected deficiencies. ICTR is already studying these recommendations and will take steps to avail itself of the external opportunities available to support ICT services. Since receiving this audit report, it has reviewed their available services and will be looking for support in the areas of Web site hosting remote access to public archives, datacenter setup, remote online backup, offsite storage, data conversion,- consulting services. The modalities will be worked out in the next few months of preparing for the next biennium budget.* Based on ICTR's response recommendation 2 has been closed.

<u>ICT risk management framework</u>

19. A risk management framework should ensure a timely identification and assessment of risks, and implementation of corresponding mitigating controls. ICTR did not implement an ICT risk management framework and had not completed a risk assessment to identify ICT risks and implement corresponding mitigating controls. While ICTR is located in a region that is subject to seismic activity, has a rift valley and is close to an active volcano, it has not undertaken a risk identification and assessment of the threats that it faced with regards to this environmental condition. The lack of a proper risk assessment and mitigation plan may prevent the Tribunal from restoring and continuing its activities in case of adverse conditions.

20. *ICTR stated that it already identified this risk in the course of working on the archives of the tribunal and presented a report to the International Working Group on ad-hoc Tribunals (IWGT). The report concluded that the current storage facilities were inadequate due to the environmental factors identified in*

the audit report and proposed a purpose built facility with robust infrastructure to house the tribunal's hard copy and electronic archives in the long term. A costing plan has already been done and submitted to the Working Group. In the short term, the Local ICT Committee will assume the responsibility for developing a risk mitigation plan with BMS pending the availability of resources for a more permanent location. Based on ICTR's on-going actions, no recommendation is issued on this matter.

ICT project management standard

21. The standard project management methodology adopted by the United Nations Secretariat is "Prince-II" (Projects in Controlled Environment). Adhering to a standard project management methodology ensures that key tasks are completed in a logical and controlled order, preventing duplications and rework. ITSS had trained staff as "Prince-II" practitioners. However, there was no evidence that the locally developed applications were based on a structured project management process or structured system development life cycle (SDLC).

22. The UNHQ ICT project management framework stipulates that all new ICT investments and major enhancements with a total cost of ownership of more than $250,000 require a business case and should be channeled through the ICT project management framework for approval. ICTR started an audio-visual digitization project with an estimated cost of $10 million. Although a business case was documented, this project was not channeled through the investment governance process. ICTR also noted that the audio visual project mentioned in the audit observation was implemented prior to the UNHQ ICT project management framework and could no have been channeled through the framework. However, the project is largely being managed in accordance with Prince2 methodology.

23. *ICTR further stated that it has already invested in capacity building and trained several ICT staff in the implementation of Prince-II methodology in the last biennium. This will enable the Tribunal to formally implement Prince-II project management methodology according to established OICT guidelines.*. Based on ICTR's assurances, no recommendation is issued on this matter.

B. ICT Operations

ICT capacity management

24. Standard ICT operational procedures should be documented for the configuration, integration and maintenance of hardware and infrastructure software. ITSS did not have adequate documented procedures in place to support ICT operations and address the challenges and risks presented by the ageing infrastructure and capacity limitations presented by the completion strategy. Although a partial rationalization of resources was implemented (e.g. use of shared network printers), ICTR lacked a formal and documented plan to address the risks represented by:

(a) Inadequate server capacity and the use of first generation servers with: (i) constant performance degradation (server downtime, systems unavailability) problems resulting in divisions having to procure and maintain their own servers; and (ii) limited hardware storage capacity resulting in limited log retention for monitoring and audit trail purposes; and

(b) Development, test and production environments that were not adequately segregated.

25. ICTR had in operation legacy applications that were no longer supported by developers and there was no evidence of a strategy or plan for maintaining /upgrading these applications, including:

(a) Analysis of the options available with regard to the use or termination of existing legacy applications; and

(b) Collaboration with other United Nations entities (i.e. Department of Field Support) on surplus equipment/tools that may be of benefit to the Tribunal.

26. OIOS observed that the following applications were currently experiencing performance degradation issues:

(a) Mercury application developed by the Department of Field Support (DFS), and used by the Procurement Unit was still in version 1.1, whilst the version currently supported by DFS was version 6 and above. The Procurement Unit was unable to perform essential processes and generate required reports; and

(b) The Field Assets Control System (FACS), which was also a DFS developed inventory application, had not been used by DFS in over 4 years. The application was no longer supported by DFS and was subject of constant losses of data.

Recommendation 3

(3) ICTR should: (a) Document procedures and guidelines for the configuration, integration and maintenance of hardware and infrastructure software; and (b) Develop a plan for the rationalization, acquisition and upgrade of the technology infrastructure in alignment with the requirements of its completion strategy.

27. *ICTR accepted recommendation 3 stating that a process for implementation of the industry standard Information Technology Infrastructure Library (ITIL) is envisaged to be undertaken by the local ICT Committee. Where necessary, ICTR plans to liaise with other United Nations entities in charting a way forward. The process for developing an ICT acquisition plan and a formal ICT resource lifecycle management plan is envisaged to be undertaken by the*

local ICT Committee. Resources required for infrastructure upgrades will be included in the 2012-13 biennium budget. Recommendation 3 remains open pending receipt of: a) documented procedures and guidelines for the configuration, integration and maintenance of hardware and infrastructure software; and b) the plan for rationalization, acquisition and upgrade of the technology infrastructure.

Bandwidth capacity

28. Capacity management procedures should ensure that bandwidth resources are adequately managed, monitored and allocated. The ICTR network was subject to near capacity bandwidth utilization. ITSS did not implement a strategy for streamlining the use of bandwidth resources and develop a systematic process for prioritization of bandwidth allocation. It also did not have adequate tools to effectively monitor usage and to determine future capacity requirements. In addition, ICTR faced problems with bandwidth availability due to limitations in the offering of commercial services within its geographical location. OIOS analyzed bandwidth utilization over a three day period and observed that on all three days the bandwidth was being used to maximum capacity.

29. Some of the consequences of the bandwidth limitations included:

(a) Hindrance to the implementation of an automated backup process and limited ability for automating data transfer across the network;

(b) Lack of public access to the records management system (TRIM) containing the judicial records database. This application was also the main access to information available to the defence counsel; and

(c) Complaints about the need to prolong the presence of staff in the office for performing data transfers (e.g. payroll EFT transactions).

Recommendation 4

(4) ICTR should undertake an analysis of its bandwidth requirements to streamline the use of its resources, and develop a systematic process for the prioritization of bandwidth allocation. This process should be implemented in accordance with quality of services criteria for monitoring network traffic flows and patterns.

30. *ICTR accepted recommendation 4 stating that ITSS/EDP has already procured bandwidth optimization software with implementation envisaged within the first quarter of 2011.* Based on ICTR's response, recommendation 4 has been closed.

UNDF communication links and archiving procedures

31. Effective communication links are critical to the operations of the United Nations Detention Facility (UNDF). UNDF is located approximately 5 miles from the Tribunal and was connected to the Tribunal's main network via end-to-end radio links. However, UNDF faced regular transmission interruptions causing loss of communication for Internet, telephone and fax. OIOS was informed that these interruptions sometimes lasted for weeks. This was a critical problem since it limited the ability of detainees to communicate with their lawyers and could potentially be seen has a limitation of their rights.

32. In addition, UNDF did not have access to the records management system "TRIM" and to tools for scanning and archiving sensitive information. UNDF maintained sensitive records going back to 1996 in safes and filing closets. Also, UNDF had no back-up system for the records it maintained. This condition exposed UNDF to risks of loss and unauthorized access to sensitive data.

Recommendation 5

(5) ICTR should: (a) Review the communication requirements of the United Nations Detention Facility and implement secure and operational communication links; and (b) Implement data storage and archiving procedures for the United Nations Detention Facility by providing access to secure storage facilities and the TRIM application.

33. *ICTR accepted recommendation 5 stating that ITSS/EDP has submitted technical specifications to the Procurement Section for initiating the tendering process of a dedicated link to UNDF. The implementation date will depend on the procurement of necessary equipment. As part of its overall strategy to develop a coordinated approach to the management of archives and records, ICTR formed the Archives and Records Management Working Group (ARMWG). The terms of reference of this working group includes facilitation of development of retention, classification and access policies for all records of the ICTR. The working group has been working with an appointed focal point of the UNDF. The focal point has already produced a records inventory to guide retention and classification of UNDF records. ICTR is also working on the development of standard policies on data storage and archiving procedures and the implementation of TRIM at the detention facility can easily be achieved upon the installation of the dedicated link mentioned above.* Based on ICTR's response, recommendation 5 has been closed.

Service management procedures

34. ICT service management procedures should enhance operational effectiveness by defining, monitoring and measuring ICT services and aid the delivery of service provision. In this regard, best practices recommend the development of ICT service catalogues documenting standard services and

deliverables, and service level agreement (SLA) defining expectations and metrics for measuring performance indicators.

35. ITSS did not have adequate procedures in place for managing the provision of its services, including: (a) Undefined incident management and event reporting procedures; (b) Lack of configuration, release, quality assurance and change management procedures; (c) Undocumented risk assessment procedures; and (d) lack of automated tool for service desk management. These control weaknesses expose ICTR to risks that could lead to unauthorised changes, ineffective and inconsistent use of resources, and inability to prevent security incidents.

36. Although ITSS had trained some of its staff in the industry standard for service management and delivery (Information Technology Infrastructure Library, ITIL), there were not established procedures and processes in line with the ITIL requirements for service delivery.

Recommendation 6

(6) ICTR should: (a) Develop ICT service processes and document service procedures in line with best practices for service delivery (i.e. ITIL), including service, performance and capacity management programmes; and (b) Deploy an automated tool for supporting service desk management, including monitoring and collection of operational data for reporting purposes.

38. *ICTR accepted recommendation 6 stating that implementation of ITIL across the Tribunal is envisaged to be undertaken by the local ICT Committee. ITSS/EDP has implemented a service desk management based on a commercial off-the-shelf software (Track-IT!). The analysis of operational data from this system will establish necessary benchmarks and indicators for service delivery.* Based on ICTR's response, recommendation 6 has been closed.

<u>Asset and inventory management procedures</u>

39. ICT assets should be held securely and managed throughout their lifecycle (from purchase to final disposition) using adequate asset management procedures.

40. ICTR did not document local asset management procedures and guidelines establishing criteria for the classification and handling of ICT assets (particularly sensitive data) managed and supported by ITSS. In addition, there were no mechanisms in place to prevent the connection of non-standard assets to the ICTR network.

41. ITSS had the highest number of missing equipment within the Tribunal. The reported causes of this condition included: a) Theft; b) Allocation of assets to users without record keeping; and c) Moving of assets between locations

without record keeping. Also, ICTR did not use tamper proof bar coding for desktop assets.

42. ICTR did not have adequate procedures for writing off ICT equipment. ITSS held 120 items of equipment waiting to be written off and the ITSS asset discrepancy list contained 305 items of equipment missing as far back as 1999. Some of the equipment were past their useful economic life and may no longer be useable.

Assets missing for more than 2 years

Years	No. of items
>2<4	46
>4<6	49
More than 6	14

43. ICTR did not document a disposal policy on ICT equipment to ensure:

(a) The secure removal of data from storage media held on obsolete and damaged equipment; and

(b) The disposal of toner cartridges. OIOS observed that due to environmental considerations, used toner cartridges were kept in a container indefinitely without any plan for disposal.

44. ICTR faced challenges in ensuring the security of ICT assets due to physical security limitations. These limitations resulted from the sharing of premises with external organizations and the existence of several exit points from the premises. OIOS noted that the ITSS warehouses (EDP and COMMS) were located in a basement that could be accessed and exited via areas not leased by the Tribunal.

Recommendations 7 and 8

ICTR should:

(7) Document local asset management procedures and guidelines to ensure the security, allocation and monitoring of ICT assets. These procedures should: (a) include provisions for determining a cut-off date for ICT equipment on the missing list, and request a waiver to enable the administrative write-off of the equipment that have exceeded their useful economic or operational life; and (b) define a disposal policy on ICT equipment and ensure that the policy covers adequate arrangements for the secure disposal of removable media and the disposal of used toner cartridges; and

(8) In collaboration with the Department of Safety and Security, review the physical security arrangements of ICT

equipment and document a strategy to safeguard ICT resources and assets (e.g. locations of CCTV cameras, ITSS warehouses).

45. *ICTR accepted recommendation 7 stating that ICT assets are issued to individual and collective end-users in ICTR. The programme manager of the end-users signs the vouchers of assets assigned for the purposes of accountability. ICT assets are stored in secured storage facilities. The storage facilities are under 24 hour surveillance by Security and Safety Services Section. Records of missing ICT equipment are currently being updated with a view to initiating administrative write-off requests which will lead to write-off of such equipment and their removal from active inventory of ICT records, following the approval of the respective Boards of Survey. This exercise is expected to be completed by 01 June 2011. EDP is leading the exercise on the write-off of missing property under their management. The cut off date for non- expendable property including some ICT assets is five years and above. However, this procedure has been hampered by lack of financial resources to replace equipment which has exceeded useful life span. This activity will be included in the planning budget for the next biennium. As the completion strategy imposes a reduction in staffing, ICTR will commence implementation within the current year. Disposal of ICT equipment is determined by the Local Property Survey Board. Used toner cartridges are being advertised for "sale as is" to avoid delays in their disposal. Procurement Section could not secure a systems contractor to purchase and remove used toner cartridges from ICTR premises. Buyers will be advised in the bills of sale to dispose used toner cartridges in accordance with environmental policy guidelines of the host country. ICT equipment has also been donated to Government institutions in Arusha. In the United Nations Peacekeeping Missions, communications equipment which becomes obsolete or damaged beyond economical repair is usually destroyed. Government institutions requesting donations of ICT equipment in Arusha are informed on the condition of the items before the equipment is released to the recipients.* Based on ICTR's response recommendation 7 has been closed.

46. *ICTR accepted recommendation 8 stating that the development of an overall strategy pertaining to physical safeguards of ICT equipment is envisaged to be undertaken by the Local ICT Committee.* Recommendation 8 remains open pending documentation of a strategy to safeguard ICT resources and assets within the Tribunal.

C. Information security management

Information security officer and procedures

47. An information security officer should be responsible for the identification of information risks and the development and implementation of standards and control procedures within the Tribunal. ICTR did not have a dedicated information security officer and lacked a formalized ICT security awareness and vulnerability management process. The information security function was performed in an ad-hoc manner by the network administrator. In addition, independent assessments of information security risks were not

performed. In this condition the Tribunal may be unable to prevent and respond to security incidents and incur in the loss of sensitive data.

48. High level ICT security policies should be complemented by local procedures and guidelines for providing direction to staff on how to securely use systems and applications and to protect sensitive data. OIOS observed that there were: (a) Inconsistent application of standards for security of ICT operations and data management; and (b) No central oversight to ensure the security and integrity of the ICT systems and data contained within systems and applications. In addition, ICTR lacked mechanisms to ensure strong authentication, protection of desktop computers and mobile devices (i.e. laptops) with updated antivirus applications. OIOS also observed the use of 'strip' shredders for disposing sensitive and confidential documents. 'Strip' shredders cut paper in long strips whereby confidential documentation could still be reassembled.

Recommendation 9

(9) ICTR should: (a) Develop and implement local information security policies and procedures in accordance with the standard adopted by the United Nations Secretariat (ISO 27001); and (b) Appoint a dedicated information security officer reporting to the Chief of Administration to manage the implementation of a comprehensive risk-based information security programme.

49. *ICTR accepted recommendation 9 stating that it will be addressed in the 2012-2013 budgets for ICTR and the Residual Mechanisms. In the short term, ITSS/EDP will work with OTP to review, draft and implement computer security vulnerability management process; subsequently, the security vulnerability process will be assumed by the Information Security Officer. ICTR has also implemented a dual Anti-Virus (AV) scenario for all computers with definitions and updates centrally managed with monitoring procedures in place. ITSS/EDP will undertake a review exercise pertaining to workstation and laptop security as part of the computer vulnerability process.* Recommendation 9 remains open pending implementation of local information security policies, the appointment of a dedicated information security officer and the implementation of a vulnerability management process.

Disaster recovery and business continuity procedures

50. Disaster recovery and business continuity (DRBC) planning should define how the organization will respond in case of adverse conditions, ensuring its ability to maintain continuity of processes and recovery of data. An inadequate plan may result in the failure to recover systems and services in a timely manner, loss of data and unavailability of critical ICT resources.

51. ICTR documented a disaster recovery and business continuity plan (DRBC). However, the plan was not completed with: (a) off-site locations for redundancy of critical ICT systems and disaster recovery testing; (b) secure off-

site storage facilities for back- up tapes; and (c) adequate protection from malicious code as part of its DRBC process.

Recommendation 10

(10) ICTR should complete its disaster recovery and business continuity processes and procedures by: (a) Documenting and implementing a back-up strategy; (b) Implementing a disaster recovery hot site and performing regular disaster recovery and business continuity tests; and; (c) Moving backup tape storage offsite to ensure effective disaster recovery.

52. *ICTR accepted recommendation 10 stating that ITSS/EDP has initiated a review of the existing DR/BC plan including conducting regularly scheduled tests. A "cold site" for disaster recovery currently exists and there is a plan for upgrading the existing site to a "hot site". In addition, a secure offsite location will be sourced for storage of backup tapes. During the meeting of the Joint Archives Strategy Working Group at The Hague, ICTR proposed to ICTY to exchange backup tapes for securing data stored in both locations. The modalities for implementation will be addressed in due course. The ICTR will avail itself of the opportunities provided by the International Computing Centre by initiating contacts and developing an action plan for areas where assistance is required.* Recommendation 10 remains open pending implementation of the disaster recovery site and backup procedures.

Records archiving

53. Core documentation of the Tribunal's activities includes its judicial records that were stored both manually and digitally. Regardless of the form in which the records were maintained, policies and evaluation mechanisms should be in place to ensure that all records comply with the requirements for retention, security and access.

54. *ICTR stated that sensitive judicial records have already been classified and archived with different levels of sensitivity clearly identified. With respect to administrative records, the ICTR will be implementing provisions of the classification levels already in use by ARMS. The development of archives and records management guidelines and procedures were important topics of discussion at the joint Tribunals Archival Strategy Working Group meeting held in The Hague on 8 and 9 of February. A significant outcome of that meeting was the development of a way forward in the establishment of an access and security regime for the non judicial substantive records such as those found within OTP and the Registry's judicial and legal services function. Work is well underway with ICTY to produce a security and access regime. A draft Secretary-General Bulletin is in circulation which will be reviewed by UNARMS and OLA. According to Resolution 1966 creating the Residual Mechanism, the records of the ICTR will not be transferred to UNARMS but rather will remain in Arusha, permanently.* Based on ICTR's response, no recommendation is issued on this matter.

Information architecture and data classification

55. Information architecture is a conceptual framework that defines the flow of information and the basic structure, content, and relationships of the applications and systems employed by an organization to process the data needed in support of its activities. This framework also enables the classification of data based on their criticality and sensitivity.

56. Parts of the Tribunal, such as OTP and CMS had partially documented their data classification standards and procedures for judicial records. However, these standards were not consistently applied across the various areas of the Tribunal and did not include the common storage of records and archives. The Tribunal's data and information had not been classified in accordance with the classification policy of the United Nations Secretariat (ST/SGB/2007/6 Information Sensitivity, Classification and Handling). Causes of this condition were attributed to: (a) The absence of an information architecture for acquiring, managing, using and storing data throughout the Tribunal; and (b) The lack of a dedicated resource responsible for the implementation and standardization of a data classification schema across the Tribunal.

57. Professional standards recommend that users with access to sensitive data be required to sign a disclosure of information and confidential statements for preserving the confidentiality of the data in their stewardship. In this regard, OIOS observed that the users of the Tribunal's applications holding sensitive information (i.e. TRIM and ZYLAB) were not required to sign disclosure of information and confidentiality statements, exposing ICTR to risks of unauthorized access to sensitive data.

Recommendation 11

(11) ICTR should develop an information architecture and implement a standard data classification schema, including documenting procedures that ensure: (a) The application of standards across the Tribunal for the common storage of records and archives; (b) The integrity and consistency of data stored in electronic form; and (c) The implementation of procedures ensuring that users with access to sensitive data are required to sign a disclosure of information and confidentiality statements.

58. *ICTR accepted recommendation 11 stating that within the scope of its Archives and Records management Working Group, policies on data classification, retention and preservation for all ICTR substantive records are being developed for review by OLA, UNARMS and ICTY. Once approved, the guidelines will be implemented. The conditions of ST/SGB/2007/6 will continue to apply to administrative records. As part of the completion strategy, the ARMWG is conducting an inventory of electronic records across the various organs of the Tribunal with a view to using existing institutional memory to produce adequate documentation. ICTR and ICTY have a joint project. ICTR will be recruiting an electronic records specialist to assist in developing a unified*

strategy on the management and preservation of electronic records and other migration issues that might arise when the Tribunal will adopt a common approach to archiving. The OTP has started using a database for documenting its systems setup. ICTR will explore the possibility of expanding the practice to EDP. Information in ICTR databases is classified into various levels wherein access is role based. The judicial records maintained in the TRIM database already are classified in accordance with ST/SGB/2007/6. To strengthen security, ICTR will implement a protocol for users to sign disclosure of information and confidentiality statements before accessing sensitive information. ICTR is working on designing a document that will be common to all ICTR staff. Recommendation 11 remains open pending the implementation of the initiative started by ICTR for the development of classification guidelines, inventory of electronic records and the unified storage strategy.

Access control management

59. Professional security management standards (i.e. ISO 27001) recommend that secure areas should protected with appropriate entry controls to ensure that only authorized personnel are allowed access.

60. ICTR had two primary server rooms and a back-up server room. Access to the primary server rooms was granted to users holding pre-coded ID badges. OIOS obtained an access log for the server room and identified instances where access into the server room was granted to staff using access cards associated with users who had departed from the Tribunal.

61. ICTR did not have adequate procedures for complementing the policies on the use of ICT resources centrally issued by the United Nations Secretariat. The "checking out" procedures established in ICTR did not contain the requirement for ensuring that important records/sensitive data and assets are handed over on departure of the staff member from the Tribunal. OIOS compared checkout reports provided by the human resource unit of ICTR unit for the period 01 Jan 2009 - 31 Dec 2009, against the list of active users (extracted from the Windows active directory server), and identified that 46 of the 52 (88 percent) staff members that departed ICTR in 2009 had active user accounts. In addition, OIOS identified that the accounts of staff that had left the Tribunal were still active on its critical applications (ZYLAB and TRIM), due to ineffective communication between HR and ITSS.

62. In addition, there were a significant number of available unsecured wireless access points within the ICTR shared environment, allowing ICTR staff to deliberately or accidentally connect to the Internet, thereby bypassing ICTR network security controls. This condition presented a risk of unauthorized access to the ICTR network and data.

Recommendation 12

(12) ICTR should: (a) Develop and implement an access control management policy in accordance with the template and procedures established in UNHQ, and perform regular

reviews of user access to all critical servers, applications, services, deleting user accounts that are no longer required; (b) Ensure that records/sensitive data and assets are handed over on departure of the staff member; (c) Remove access rights of all users (staff, contractors and third party users) upon termination of their employment, contract or agreement; and (d) Address the security requirements of all wireless access points available in the campus.

63. *ICTR accepted recommendation 12 stating that physical security enhancements of the ICTR data center will be undertaken in conjunction with the Building Management and Security Sections. The development and implementation of standard access control policies across the Tribunal is envisaged to be undertaken by the Local ICT Committee. ITSS/EDP/OTP will disable wireless interfaces on laptops and workstations, considering also that disabling wireless interfaces will not solve all security issues as Internet can be accessed with USB devices. As a supplement, an official advisory will be published to staff to sensitize users to security implications.* Based on ICTR's response, recommendation 12 has been closed.

Application security

64. ICT applications should have embedded controls for ensuring the security, reliability and integrity of data. These controls should include access control mechanisms and database integrity controls based on the functional processes.

65. OIOS undertook a review of two critical applications used in ICTR: (i) A records management system (trim); and (ii) An investigation and case management suite containing highly sensitive documents (ZYLAB)). The results of the audit review highlighted the following control weaknesses:

TRIM application

(a) ICTR implemented a 'single sign-on' capability for the TRIM application, whereby, access is granted to users on the basis of the ICTR network identification and passwords. However, there were a number of dormant user identities assigned to staff members that have departed from the organization and had not been removed (from the Windows Active Directory Server). This condition could result in unauthorized access to highly sensitive information contained within the TRIM application; and

(b) There were fifteen administrator user accounts in TRIM, with a majority of them having the highest level of security access. OIOS observed that some of the administrator accounts were associated to generic profiles that could have been used by anyone. This condition exposed the Tribunal to the risk of users

bypassing access controls, change system and security settings, modify logins and user profiles, and delete/purge documents.

ZYLAB application

(a) The Office of the Prosecution (OTP) had enabled a password security policy for the ZYLAB application. However, the password complexity requirements had been disabled making the application more vulnerable to security breaches using password cracking software or social engineering; and

(b) The default built-in administrator account (with the highest level of permissions on the application) was renamed and used by a system user.

Recommendation 13

(13) ICTR should enhance the access controls embedded in the TRIM and ZYLAB applications.

66. *ICTR accepted recommendation 13 stating that OTP/ZYLAB password complexity feature is now enabled. CMS is in the process of reviewing all user accounts and is deactivating those of departed staff member. The number of administrator accounts in TRIM has now been decreased to nine, all of which are associated with an individual user, either in CMS or EDP. All users with administrator rights require those rights to perform their functions.* Based on ICTR's response, recommendation 13 has been closed.

Physical and environmental security of ICT resources

67. Information security standards (i.e. ISO 27001) recommends the design and implementation of physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disasters.

68. OIOS undertook a verification of the physical and environmental security of the Tribunal's ICT installations and observed the following:

(a) Unsecured glass window in the back end of the main server room "K105C" (data center), making the data centre easily accessible;

(b) Insufficient number and inadequate placement of cameras for monitoring;

(c) The backup server room was in a container lacking fire suppression system, security cameras and badge access controls; and

(d) Although the main server room "K105C" was equipped with fire suppression system installed in the ceiling of the room, there was a need to improve the positioning of the fire extinguishers.

Recommendation 14

(14) ICTR should strengthen the current physical security controls of its ICT installations by: (a) Replacing the back end glass window with concrete wall; (b) Installing CCTV cameras inside and outside; and (c) Mounting all fire suppression systems.

69. *ICTR accepted recommendation 14 stating that physical security enhancements of the ICTR data center will be undertaken in conjunction with the Building Management and Security Sections.* Recommendation 14 remains open pending enhancements to the physical security of ICT installations.

V. ACKNOWLEDGEMENT

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

ANNEX 1

STATUS OF AUDIT RECOMMENDATIONS

Recom. no.	Recommendation	Risk category	Risk rating	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
1.	ICTR should: (a) Document a formal ICT strategy to define how ICT services will contribute and support the Tribunal. The strategy should take into consideration the need to ensure continuous provision of ICT services and support until the completion of Tribunal's activities; and (b) Establish an ICT steering committee comprising representatives of the Tribunal's major stakeholders	Governance	Medium	O	Establish a local ICT committee and document a formal ICT strategy.	April 2011
2.	ICTR should: (a) Review its budget structure and ensure transparency of all ICT associated costs across the Tribunal; (b) Document and periodically review its human resources plan and ICT staffing requirements, ensuring that they are aligned with the Tribunal's completion strategy; (c) Maximize existing ICT resources and undertake a rationalization exercise of existing ICT staffing resources and equipment within ITSS, the Office of the Prosecution & Court Management Services; and Consider the use of the services provided by the International Computing Centre and United Nations Volunteers to provide staffing resources in support of ICT service requirements	Information/HR resources	Medium	C		June 2011/January 2012

Recom. no.	Recommendation	Risk category	Risk rating	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
3.	ICTR should: (a) Document procedures and guidelines for the configuration, integration and maintenance of hardware and infrastructure software; and (b) Develop a plan for the rationalization, acquisition and upgrade of the technology infrastructure in alignment with the requirements of its completion strategy.	Governance/Information resources	Medium	O	Document procedures and guidelines for the (a) configuration, integration and maintenance of hardware and infrastructure software and (b) Develop a plan for rationalization, acquisition and upgrade of the technology infrastructure.	June 2011
4.	ICTR should undertake an analysis of its bandwidth requirements to streamline the use of its resources, and develop a systematic process for the prioritization of bandwidth allocation. This process should be implemented in accordance with quality of services criteria for monitoring network traffic flows and patterns.	Information resources	Medium	C		April 2011
5.	ICTR should: (a) Review the communication requirements of the United Nations Detention Facility and implement secure and operational communication links; and (b) Implement data storage and archiving procedures for the United Nations Detention Facility by providing access to secure storage facilities and the TRIM application.	Information resources	High	C		June/September 2011
6.	ICTR should: (a) Develop ICT service processes and document service procedures in line with best practices for service delivery (i.e. ITIL), including service, performance and capacity management programmes; and (b) Deploy an automated tool for supporting service desk management, including monitoring and	Information resources	Medium	C		

Recom. no.	Recommendation	Risk category	Risk rating	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
	collection of operational data for reporting purposes.					
7.	ICTR should document local asset management procedures and guidelines to ensure the security, allocation and monitoring of ICT assets. These procedures should: (a) include provisions for determining a cut-off date for ICT equipment on the missing list, and request a waiver to enable the administrative write-off of the equipment that have exceeded their useful economic or operational life; and (b) a disposal policy on ICT equipment and ensure that the policy covers adequate arrangements for the secure disposal of removable media and the disposal of used toner cartridges	Information resources	Medium	C		June 2011
8.	ICTR, in collaboration with the Department of Safety and Security, should review the physical security arrangements of ICT equipment and document a strategy to safeguard ICT resources and assets (e.g. locations of CCTV cameras, ITSS warehouses).	Information resources	Medium	O	Document a strategy to safeguard ICT resources and assets within the Tribunal.	June 2011
9.	ICTR should: (a) Develop and implement local information security policies and procedures in accordance with the standard adopted by the United Nations Secretariat (ISO 27001); and (b) Appoint a dedicated information security officer reporting to the Chief of Administration to manage the implementation of a comprehensive risk-based information security programme.	Information resources	Medium	O	Implement local information security policies, appoint a dedicated information security officer and implement a vulnerability management process.	June/August 2011

Recom. no.	Recommendation	Risk category	Risk rating	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
10.	ICTR should complete its disaster recovery and business continuity processes and procedures by: (a) Documenting and implementing a back-up strategy; (b) Implementing a disaster recovery hot site and performing regular disaster recovery and business continuity tests; and; (c) Moving backup tape storage offsite to ensure effective disaster recovery.	Information resources	High	O	Implement the requirements of recommendation 12.	March/June 2011
11.	ICTR should develop an information architecture and implement a standard data classification schema, including documenting procedures that ensure: (a) The application of standards across the Tribunal for the common storage of records and archives; (b) The integrity and consistency of data stored in electronic form; and (c) The implementation of procedures ensuring that users with access to sensitive data are required to sign a disclosure of information and confidentiality statements.	Information resources	Medium	O	Provide copy of the classification guidelines, inventory of electronic records and unified storage strategy.	June 2011
12.	ICTR should: (a) Develop and implement an access control management policy in accordance with the template and procedures established in UNHQ, and perform regular reviews of user access to all critical servers, applications, services, deleting user accounts that are no longer required; (b) Ensure that records/sensitive data and assets are handed over on departure of the staff member; (c) Remove access rights of all users (staff, contractors and third party users) upon termination of their employment, contract or agreement;	Information resources	Medium	C		June 2011

Recom. no.	Recommendation	Risk category	Risk rating	C/ O[1]	Actions needed to close recommendation	Implementation date[2]
	and (d) Address the security requirements of all wireless access points available in the campus.					
13.	ICTR should enhance the access controls embedded in the TRIM and ZYLAB applications.	Information resources	Medium	C		Not provided
14.	ICTR should strengthen the current physical security controls of its ICT installations by: (a) Replacing the back end glass window with concrete wall; (b) Installing CCTV cameras inside and outside; and (c) Mounting all fire suppression systems.	Information resources	Medium	O	Enhance the physical security of ICT installations.	September 2011

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