



INTERNAL AUDIT DIVISION

REPORT 2016/068

Audit of archives and records management at the Mechanism for International Criminal Tribunals

Overall results relating to the management of archives and records were initially assessed as partially satisfactory. Management has satisfactorily implemented the audit recommendations.

FINAL OVERALL RATING: SATISFACTORY

13 June 2016
Assignment No. AA2016/261/01

CONTENTS

	<i>Page</i>
I. BACKGROUND	1-2
II. OBJECTIVE AND SCOPE	2
III. AUDIT RESULTS	2-6
A. Strategic planning and risk assessment	3-4
B. Regulatory framework	4-6
IV. ACKNOWLEDGEMENT	6
ANNEX I Status of audit recommendations	
APPENDIX I Management response	

AUDIT REPORT

Audit of archives and records management at the Mechanism for International Criminal Tribunals

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of archives and records management at the Mechanism for International Criminal Tribunals (MICT).
2. In accordance with its mandate, OIOS provides assurance and advice on the adequacy and effectiveness of the United Nations internal control system, the primary objectives of which are to ensure (a) efficient and effective operations; (b) accurate financial and operational reporting; (c) safeguarding of assets; and (d) compliance with mandates, regulations and rules.
3. MICT was established by United Nations Security Council resolution 1966 on 22 December 2010 to carry out a number of essential functions of the International Criminal Tribunal for Rwanda (ICTR) and the International Criminal Tribunal for the former Yugoslavia (ICTY), after the completion of their respective mandates.
4. In accordance with its statute, MICT is responsible for the management, preservation and provision to both internal and external users' access to the ICTR, ICTY and its own archives. The archives document MICT and Tribunals' investigations, indictments and court proceedings, their work relating to the detention of accused persons, the protection of witnesses and enforcement of sentences, and their relationships with states, other law enforcement authorities, international and non-governmental organizations and the general public. The archives consist of documents, maps, photographs, audiovisual recordings and objects. MICT preserves these materials and facilitates the widest possible access to them while ensuring the continued protection of confidential information.
5. The Arusha branch of MICT is home to ICTR archives, which holds nearly 2,000 linear meters of physical records and one petabyte of digital records. ICTY archives are located at The Hague branch of MICT, estimated at 10,000 linear meters of physical records and two petabytes of digital records.
6. The Mechanism's Archives and Records Section (MARS), which is part of the Registry, manages the archives and provides guidance on the management of records in MICT. MARS archives are co-located with the respective branches of MICT in Arusha and The Hague. MARS' responsibilities include developing and implementing strategies, policies and procedures to ensure the preservation of Tribunal archives and the provision of appropriate access to them. MARS also provides advice and guidance to ICTR and ICTY on the preparation and transfer of their archives. In this regard, MARS has issued standards for the preparation and transfer of both physical and digital records, besides providing training to assist Tribunal staff in implementing these standards
7. In The Hague branch, the section is headed by the Chief Archivist, at the P-5 level, who reports to the Deputy Registrar, while in the Arusha branch, it is headed by the Head of MARS – Arusha, at the P-4 level, who reports to the Officer-in-Charge of the Division of Registry and to the Chief Archivist as an Additional Reporting Officer. Both the Deputy Registrar and the Officer-in-Charge report to the Registrar. MARS has 22 staff members overall, with 11 positions based in The Hague and 11 in Arusha. In the 2014-2015 biennium, its projected final expenditure was \$8.9 million, with \$4.8 million for The Hague office and \$4.1 million for Arusha.

8. Comments provided by MICT are incorporated in italics.

II. OBJECTIVE AND SCOPE

9. The audit was conducted to assess the adequacy and effectiveness of MICT governance, risk management and control processes in providing reasonable assurance regarding **effective management of archives and records at MICT**.

10. This audit was included in the 2015 internal audit work plan for MICT due to the significant risks associated with the management of archives and records.

11. The key controls tested for the audit were: (a) strategic planning and risk assessment; and (b) regulatory framework. For the purpose of this audit, OIOS defined these key controls as follows:

- (a) **Strategic planning and risk assessment** - controls that provide reasonable assurance that an appropriate strategy is in place for managing archives and records, and that the related risks are assessed and mitigated effectively; and
- (b) **Regulatory framework** - controls that provide reasonable assurance that: (i) policies and procedures exist to guide MICT on effective management of the archives and records; (ii) are implemented effectively; and (iii) ensure the reliability and integrity of operational information.

12. The key controls were assessed for the control objectives shown in Table 1.

13. OIOS conducted the audit from 15 February to 31 March 2016. The audit covered the period from 1 January 2014 to 31 March 2016.

14. OIOS conducted an activity-level risk assessment to identify and assess specific risk exposures, and to confirm the relevance of the selected key controls in mitigating associated risks. Through interviews, analytical reviews and tests of controls, OIOS assessed the existence and adequacy of internal controls and conducted necessary tests to determine their effectiveness.

III. AUDIT RESULTS

15. The MICT governance, risk management and control processes examined were initially assessed as **partially satisfactory**¹ in providing reasonable assurance regarding **effective management of archives and records at MICT**. OIOS made five recommendations to address issues identified in the audit.

16. Strategic planning and risk assessment was assessed as partially satisfactory because MICT needed to: (i) set up a clear timeline for developing and implementing all pending policies concerning archives and records management; and (ii) carry out a risk assessment at The Hague branch and regularly monitor the status of the mitigation for all the identified risks. Regulatory framework was also assessed as partially satisfactory because there was a need to: (i) store backup tapes of data at a separate location;

¹ A rating of “**partially satisfactory**” means that important (but not critical or pervasive) deficiencies exist in governance, risk management or control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

(ii) strengthen monitoring of any breach of confidentiality of classified documents; and (iii) explore printing solutions that limit exposure of confidential documents to unauthorized individuals.

17. The initial overall rating was based on the assessment of key controls presented in Table 1 below. The final overall rating is **satisfactory**² as management has satisfactorily implemented the audit recommendations.

Table 1: Assessment of key controls

Business objective	Key controls	Control objectives			
		Efficient and effective operations	Accurate financial and operational reporting	Safeguarding of assets	Compliance with mandates, regulations and rules
Effective management of archives and records at MICT	(a) Strategic planning and risk assessment	Partially satisfactory	Partially satisfactory	Partially satisfactory	Partially satisfactory
	(b) Regulatory framework	Partially satisfactory	Partially satisfactory	Partially satisfactory	Partially satisfactory
FINAL OVERALL RATING: SATISFACTORY					

A. Strategic planning and risk assessment

Need to set up a clear timeline for the completion of policy development

18. The approved budget and strategic framework of MICT for the period 1 January 2014 to 31 December 2015 stated that MARS is responsible for developing and implementing strategies, policies and procedures to ensure effective preservation of MICT archives and enhancement of their access to the public.

19. In accordance with its work plans for 2014-2015 and 2015-2016, MARS was on course to accomplishing its main operational priorities for the biennium, most notably, the time-sensitive transfer of archives and records from ICTR and ICTY to MICT. In this regard, ICTR had transferred 91 per cent of the material to MICT, with the remaining 9 per cent waiting to be transferred after the liquidation team completes its operations. ICTY was also on course to transfer 50 per cent of the records to MICT by December 2016 and the remaining 50 per cent by December 2017.

20. In its work plan for 2014-2015, MARS also identified eight high-level policies to provide the broad framework for the management of records and archives. Of these, four high-level governance documents were in draft form, i.e., (i) the recordkeeping policy, in draft since 2013; (ii) the access to information policy, in draft since 2014; (iii) standards for the arrangement and description of archival records, in draft since September 2015; and (iv) a recordkeeping metadata standard, in draft since November 2015. Although the access policy and metadata standard were expected to be issued before June 2016, MICT did not have target dates for completion of the other two documents. MARS had also prepared the retention schedules for the MICT Office of the Prosecutor, but it did not finalize the

² A rating of “**satisfactory**” means that governance, risk management and control processes are adequately designed and operating effectively to provide reasonable assurance regarding the achievement of control and/or business objectives under review.

retention schedules for the Registry or Chambers. MICT explained that it did not finalize the high-level policies because its priority was the transfer of records. However, MICT acknowledged the need for finalizing the policy documents.

(1) MICT should establish a clear timeline for developing and implementing all pending policy documents concerning archives and records management.

MICT accepted recommendation 1 and stated that it has adopted a document showing realistic timelines for the development of the high-level policies and strategies. These documents will be completed in September 2018. This timeline is based, inter alia, on the following considerations: the innovative nature of these instruments within the United Nations system, the specific complexities of judicial records, the review process and approval by all three Organs of the Mechanism, existing time-sensitive operational priorities, such as the transfer of records from the ICTY before its closure, as well as the existence of governance documents which ensure the day-to-day management of the archives. Based on the action taken by MICT, recommendation 1 has been closed.

Need for The Hague branch of MARS to conduct a risk assessment and develop a risk register

21. The United Nations Policy Framework for Enterprise Risk Management and Internal Control requires MICT to proactively identify and manage risks that threaten the achievement of its objectives.

22. MARS Arusha branch had carried out a risk assessment and put in place a comprehensive and regularly-updated system for managing risks. The Hague branch of MARS had carried out an assessment of risks that could affect the transfer of records from ICTY to MICT, which it said was the most significant risk it faced. However, it was yet to assess other risks such as those pertaining to archives already transferred to it, and also those pertaining to records generated by the MICT Hague branch. There was a need to develop a comprehensive risk assessment for The Hague branch similar to the one developed by the Arusha branch in order to ensure coherence across branches, while also taking into consideration differences between the branches.

(2) The MICT Archives and Records Section should carry out a risk assessment at The Hague branch and regularly monitor the status of mitigation measures for the identified risks.

MICT accepted recommendation 2 and stated that it has conducted a risk assessment for the MICT Archives and Records Section, Hague branch. The results of the risk assessment have been compiled in a risk register. Management plans to regularly update the risk register every six months to reflect the identification of any new risks, as well as risk mitigation measures which have been put in place. The first review will occur in December 2016. Based on the action taken by MICT, recommendation 2 has been closed.

B. Regulatory framework

MICT relocated back-up tapes in a secure remote location

23. The ICTY and MICT information and communications technology (ICT) strategy of 2014-2017 requires that backup records should be stored at a secure remote location to minimize risk in the event of flooding. The strategy further stated the need to fully explore all options for the storage of back-up in a remote facility.

24. At The Hague, all 886 backup Linear Tape-Open (LTO) tapes containing approximately 1,400 terabytes of records were stored in the same building as the original LTO tapes. Initially, back-up LTO tapes were kept in a separate administration building but were moved to the current building in September 2015 as a temporary solution when the administration block was closed due to downsizing.

25. One of the components of the MICT business continuity and disaster recovery plan was the storage of backup data in remote locations. Although MICT was aware of the need to explore options to store its backup at a different location, it did not take steps to do so. There was a risk that original and back-up LTO tapes could be lost in the event of a fire or flooding.

(3) MICT should develop and implement mitigation measures as proposed in the ICT strategy for relocating backup tapes.

MICT accepted recommendation 3 and stated that it has moved all backup LTO tapes to a separate location. Based on the action taken by MICT, recommendation 3 has been closed.

MICT enhanced the security of classified records

26. Article 27 of the MICT Statute, provided by United Nations Security Council resolution 1966, requires MICT to ensure the continued protection of confidential information.

27. The Mechanism had established and implemented a corpus of procedures and measures in both branches to protect the confidentiality of records, which included:

- a. A comprehensive system of checks and balances comprised of several levels of review by legal officers and information managers to ensure that all incoming MICT judicial records are distributed according to their classification levels, and that only unclassified records are made accessible to the public;
- b. Conducting a thorough review of all ICTR and ICTY judicial records prior to declassifying and making them accessible to the public;
- c. Strictly enforced procedures for access to the repositories containing physical records, including by MICT staff; and
- d. Security and access control for databases and other systems containing digital records.

28. In addition, MICT established at the Arusha branch the Confidentiality Breach and Remedy Assessment (COBRA) Team, which is an inter-disciplinary Registry working group composed of the Heads of MARS, Witness Support and Protection Section and the Legal Team. The COBRA Team systematically monitored the use of ICTR and MICT Arusha records on the internet and in the media and took follow-up measures as necessary. While the COBRA team is a good practice in the management of records, there was no similar team at MARS, The Hague branch.

29. OIOS noted instances where certain classified documents could still be found on the internet. An online search by the audit team yielded three confidential documents, including the name of a protected witness. A strictly confidential statement by a protected witness was posted on three websites, alongside the real name of the witness. Another internet search showed that two classified judicial records were on another website not related to the aforementioned three. Another website was also found to have published a confidential witness statement in 2014.

30. MICT Arusha branch explained that in all of these cases, the websites did not obtain the documents through any breach in security on the part of the Mechanism, ICTR or ICTY. Although MICT was not certain about how the documents were accessed by websites that published it, the defence counsel

in one of the cases had initially published two of the above-mentioned documents alongside 127 other classified documents on a website. When MICT discovered this, it contacted the defence counsel who then removed the classified documents. In addition, MICT contacted all of the witnesses potentially affected by the unauthorized publication and stated that it was satisfied that their safety was not compromised. However, such information may have been accessed and potentially reposted by other internet users.

31. OIOS noted that security over classified documents inside MICT office premises required enhancement. The audit team observed that in some instances classified documents were left for hours at shared printers both at The Hague and in Arusha. As a mitigation measure, access to MICT corridors was monitored and restricted by the Security and Safety Section. Additionally, access to shared printers was restricted within the concerned sections of MICT. These measures notwithstanding, further enhancement of classified document security was required, since not all persons who used the shared printers were authorized to have access to every classified document printed.

(4) MICT should: (i) establish a Confidentiality Breach and Remedy Assessment (COBRA) Team at The Hague branch to constantly monitor the internet for any breach of confidentiality; and (ii) ensure effective coordination between the Arusha and The Hague branch COBRA teams.

MICT accepted recommendation 4 and stated that it has conducted the following activities: (i) established a COBRA Team at The Hague branch; (ii) a representative of the COBRA Team in Arusha held a coordination meeting with and training for the newly established COBRA Team in The Hague, covering terms of reference, working methods and investigative techniques; and (iii) The Hague COBRA Team started its work. Based on the action taken by MICT, recommendation 4 has been closed.

(5) MICT should explore printing solutions that limit exposure of confidential documents to unauthorized individuals.

MICT accepted recommendation 5 and stated that it explored possible solutions to the issue, including printing solutions. Management found that printing solutions would bear cost implications and that educational measures may offer equally, or more valuable solutions at zero cost to the Organization. To this end, Management has broadcast an awareness-raising message on information security and was planning in-person trainings. Additionally, awareness-raising signage had been affixed on the walls of the Arusha and The Hague branch offices. Based on the action taken by MICT, recommendation 5 has been closed.

IV. ACKNOWLEDGEMENT

32. OIOS wishes to express its appreciation to the Management and staff of MICT for the assistance and cooperation extended to the auditors during this assignment.

(Signed) Eleanor T. Burns
Director, Internal Audit Division
Office of Internal Oversight Services

STATUS OF AUDIT RECOMMENDATIONS

Audit of archives and records management at the Mechanism for International Criminal Tribunals

Recom. no.	Recommendation	Critical ³ / Important ⁴	C/ O ⁵	Actions needed to close recommendation	Implementation date ⁶
1	MICT should establish a clear timeline for developing and implementing all pending policy documents concerning archives and records management.	Important	C	Action completed.	Implemented
2	The MICT Archives and Records Section should carry out a risk assessment at The Hague branch and regularly monitor the status of mitigation measures for the identified risks.	Important	C	Action completed.	Implemented
3	MICT should develop and implement mitigation measures as proposed in the ICT strategy for relocating backup tapes.	Important	C	Action completed.	Implemented
4	MICT should: (i) establish a Confidentiality Breach and Remedy Assessment (COBRA) Team at The Hague branch to constantly monitor the internet for any breach of confidentiality; and (ii) ensure effective coordination between the Arusha and The Hague branch COBRA teams.	Important	C	Action completed.	Implemented
5	MICT should explore printing solutions that limit exposure of confidential documents to unauthorized individuals.	Important	C	Action completed.	Implemented

³ Critical recommendations address critical and/or pervasive deficiencies in governance, risk management or control processes, such that reasonable assurance cannot be provided with regard to the achievement of control and/or business objectives under review.

⁴ Important recommendations address important (but not critical or pervasive) deficiencies in governance, risk management or control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

⁵ C = closed, O = open

⁶ Date provided by MICT in response to recommendations.

APPENDIX I

Management Response

Management Response

Audit of archives and records management at the Mechanism for International Criminal Tribunals

Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	MICT should establish a clear timeline for developing and implementing all pending policy documents concerning archives and records management.	Important	Yes	Head of the Mechanism Archives and Records Section	Implemented	Management accepts this recommendation and has adopted a document showing realistic timelines for the development of the high-level policies and strategies listed in the audit report. The document shows the various stages of the development, review and approval process for all eight documents. The document also notes that these documents will be completed in September 2018. This timeline is based, <i>inter alia</i> , on the following considerations: the innovative nature of these instruments within the United Nations system, the specific complexities of judicial records, the review process and approval by all three Organs of the Mechanism, existing time-sensitive operational priorities, such as the transfer of records from the ICTY before its closure, as well as the existence of governance documents which ensure the day-to-day management of the archives. Management therefore requests that OIOS consider this recommendation to be fully implemented.

¹ Critical recommendations address critical and/or pervasive deficiencies in governance, risk management or control processes, such that reasonable assurance cannot be provided with regard to the achievement of control and/or business objectives under review.

² Important recommendations address important (but not critical or pervasive) deficiencies in governance, risk management or control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

Management Response

Audit of archives and records management at the Mechanism for International Criminal Tribunals

Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
2	The MICT Archives and Records Section should carry out a risk assessment at The Hague branch and regularly monitor the status of mitigation measures for the identified risks.	Important	Yes	Head of the Mechanism Archives and Records Section	Implemented	Management accepts this recommendation, and has conducted a risk assessment for the MICT Archives and Records Section, Hague branch. The results of the risk assessment have been compiled in a risk register. Management plans to regularly update the risk register every six months to reflect the identification of any new risks, as well as risk mitigation measures which have been put in place. The first review will occur in December 2016. Management therefore requests that OIOS consider this recommendation to be fully implemented.
3	MICT should develop and implement mitigation measures as proposed in the ICT strategy for relocating backup tapes.	Important	Yes	Head of the Mechanism Archives and Records Section	Implemented	Management has addressed this recommendation and relocated the backup tapes. No additional comment.
4	MICT should: (i) establish a Confidentiality Breach and Remedy Assessment (COBRA) Team at The Hague branch to constantly monitor the internet for any breach of confidentiality; and (ii) ensure effective coordination between the Arusha and The Hague branch COBRA teams.	Important	Yes	Registrar	Implemented	Management accepts this recommendation and has conducted the following activities: 1) established a Confidentiality Breach and Remedy Assessment (COBRA) Team at The Hague branch; 2) a representative of the COBRA Team in Arusha held a coordination meeting with and training for the newly established COBRA Team in the Hague, covering terms of reference, working methods

Management Response

Audit of archives and records management at the Mechanism for International Criminal Tribunals

Rec. no.	Recommendation	Critical ¹ / Important ²	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
						and investigative techniques; 3) The Hague COBRA Team started its work. Management therefore requests that OIOS consider this recommendation to be fully implemented.
5	MICT should explore printing solutions that limit exposure of confidential documents to unauthorized individuals.	Important	Yes	Registrar	Implemented	Management has addressed this recommendation and has explored and implemented measures at no additional cost to the Organization to limit exposure of confidential documents to unauthorized individuals. No additional comment.