Office of Internal Oversight Services

INTERNAL AUDIT DIVISION

REPORT 2014/029

Audit of the International Transaction Log system at the United Nations Framework Convention on Climate Change

Overall results relating to the effective management and operation of the International Transaction Log system were initially assessed as partially satisfactory. Implementation of five important recommendations remains in progress.

FINAL OVERALL RATING: PARTIALLY SATISFACTORY

29 April 2014
Assignment No. AT2013/241/01

CONTENTS

AUDIT REPORT

Audit of the International Transaction Log system at the United Nations Framework Convention on Climate Change

I. BACKGROUND

1. The Office of Internal Oversight Services (OIOS) conducted an audit of the International Transaction Log (ITL) system at the United Nations Framework Convention on Climate Change (UNFCCC).

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. The Kyoto Protocol, which was adopted in Kyoto, Japan in 1997 and entered into force in 2005, encouraged industrialized countries to commit to the stabilization of greenhouse gas emissions. For the first commitment period, known as "CP1", 38 countries agreed to abide by this protocol. These countries established authorized bodies (Registries) to perform transactions on carbon emission credits. Their emissions were tracked by the ITL system in UNFCCC. The ITL system had two main functions: (i) provide a logical communication hub which connects all the Registries, thereby enabling emissions trading; and (ii) monitor and verify the validity of transactions initiated by the Registries, according to the rules of the Kyoto Protocol.

4. The Registries in each country were responsible for the establishment and operation of their own systems (Registry Systems), which were interfaced with the ITL system through web services. Registry Systems tracked and recorded the movement of emissions rights, the holdings of Kyoto units[1], and any transactions involving them through a structure of accounts.

5. The architecture of the ITL system was split into front-end and back-end servers. The front-end provided a series of web services for the communication with the Registry Systems and a separate web user interface for ITL system administration. The back-end processed transactions and updated the database. Additionally, the ITL system was interfaced with other UNFCCC internal databases and systems (i.e., Compilation and Accounting Database, Clean Development Mechanism Information System, and Joint Implementation Information System).

6. The administrator of the ITL system was the UNFCCC Secretariat, which awarded a contract for the development, operation and support of the system to third party service providers. The ITL system was hosted in two commercially operated data centres for primary operations and backup. The third party service provider had also put in place a service desk to support the administrators of the ITL and the Registry systems.

7. Comments provided by UNFCCC are incorporated in italics.

[1] Emission targets for industrialized country parties to the Kyoto Protocol are expressed as levels of allowed emissions, or "assigned amounts". Such assigned amounts are denominated in tonnes (of CO2 equivalent emissions) known informally as "Kyoto units".

II. OBJECTIVE AND SCOPE

8. The audit was conducted to assess the adequacy and effectiveness of UNFCCC governance, risk management and control processes in providing reasonable assurance regarding the **effective management and operation of the ITL system**.

9. The audit was included in the 2013 internal audit work plan at the request of UNFCCC in view of the risk that failure to effectively manage and operate the ITL system could compromise the support provided to the 38 Registries worldwide.

10. The key controls tested for the audit were: (a) risk management mechanisms; (b) performance monitoring mechanisms; and (c) information and communications technology (ICT) support systems. For the purpose of this audit, OIOS defined these key controls as follows:

(i) **Risk management mechanisms** – controls that provide reasonable assurance that risks relating to the ITL system are identified and assessed, and that action is taken to mitigate them;

(ii) **Performance monitoring mechanisms** – controls that provide reasonable assurance that appropriate metrics are established and monitored to ensure that the ITL system operates effectively; and

(iii) **ICT support system** – controls that provide reasonable assurance that the ITL system adequately supports the needs of its users.

11. The key controls were assessed for the control objectives shown in Table 1. Certain control objectives shown in Table 1 as "Not assessed" were not relevant to the scope defined for this audit.

12. OIOS conducted the audit from 14 October to 30 November 2013. The audit covered the period January 2012 to November 2013, and also included key aspects from the inception of the ITL system which was originally implemented in 2006.

13. 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 review of the design and implementation of processes, procedures, and plans, interviews with ITL support staff, review of the ITL system, and physical inspection of data centres, OIOS assessed the existence and adequacy of internal controls and conducted audit tests to assess their effectiveness. In particular, OIOS: (i) analyzed ITL documentation; (ii) tested the effectiveness of the governance arrangements, project management, system development life cycle, design, testing and deployment; (iii) reviewed authorizations, security settings, configuration, and the ICT infrastructure of the ITL system; and (v) reviewed the effectiveness of the service provided by third party service providers.

III. AUDIT RESULTS

14. The UNFCCC governance, risk management and control processes examined were **partially satisfactory** in providing reasonable assurance regarding the **effective management and operation of the ITL system.**

15. OIOS made eight recommendations to address issues identified in the audit. UNFCCC and its third party service providers had adopted good practices for the implementation and support of the ITL

system, had dedicated and knowledgeable support and service teams, complied with the standard for information security management (ISO 27001 certification), and had extensive monitoring mechanisms in place. Controls over the physical infrastructure, backup operations, incident and problem management, and overall service desk operations were adequate. However, the following control weaknesses were identified in the overall system support: (i) the risk register did not include security related threats and the actions needed to mitigate risks; (ii) business continuity planning was partially addressed; (iii) security vulnerability assessments needed to be strengthened; (iv) automated alert mechanisms were not configured for critical activities; and (v) there were inadequacies in password controls.

16. The initial overall rating was based on the assessment of key controls presented in Table 1 below. The final overall rating is **partially satisfactory** as implementation of five important recommendations remains in progress.

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 and operation of the ITL system	(a) Risk management mechanisms	Partially satisfactory	Not assessed	Partially Satisfactory	Satisfactory
	(b) Performance monitoring mechanisms	Satisfactory	Satisfactory	Satisfactory	Satisfactory
	(c) ICT support system	Partially Satisfactory	Not assessed	Partially satisfactory	Satisfactory
FINAL OVERALL RATING: PARTIALLY SATISFACTORY					

A. Risk management mechanisms

Risk management practices required strengthening

17. Risk management is an essential activity for monitoring, evaluating, and managing the risks pertaining to all major ICT systems.

18. OIOS reviewed the risk management process established by UNFCCC for ITL. Some of the risks (i.e., business, technical and organizational risks) were identified and documented in the ITL risk register issued in February 2012. However, UNFCCC did not document a risk management policy and risk assessment procedure.

19. In particular, the following weaknesses were identified in the existing risk management practices:

(i) The security risks identified as a result of vulnerability assessments were not included in the risk register;

(ii) The status of several risks reported in the register indicated that no actions had been taken to mitigate the risks;

(iii) Actions to mitigate the risks were not always defined and assigned; and

(iv) Risks were not reviewed by the senior management of UNFCCC and were not categorized by their disposition as accepted, avoided, transferred, or treated.

20. The lack of a complete risk management process prevented the senior management of UNFCCC from proactively assessing the potential impact of the risks associated with the management and operation of the ITL system, and defining adequate responses.

(1) UNFCCC should document and implement a risk management policy for the International Transaction Log system, including formal procedures for risk assessment, risk monitoring, and mitigation plans.

UNFCCC accepted recommendation. Recommendation 1 remains open pending receipt of the risk management policy and procedures describing the risk assessment, monitoring and mitigation plans.

The business continuity plan was incomplete

21. A business continuity plan should define how an organization intends to respond to unexpected internal and external threats, with instructions and activities related to the expected actions of all parties responsible for ensuring the continuation of operations under adverse conditions.

22. The business continuity arrangements for ITL were inadequate because there was only one business continuity plan prepared by the third party service provider supporting the system. There were no specifications of the actions that UNFCCC ITL staff would be required to perform for ensuring the continuity of the system. At the time of the audit, UNFCCC was working on an overall organizational business continuity plan that would have also included ITL operations. However, this plan was not expected to be in place for several months. In the interim, there were several risks that could negatively affect UNFCCC's ability to ensure the continuity of ITL, as follows:

(i) UNFCCC planned a re-tendering exercise for the support of ITL services in 2015. This exercise could result in transferring the supporting responsibilities of the existing ITL services and infrastructure to a new vendor. However, there was no business impact analysis performed on the risks associated with the possible transition of the system support to another vendor;

(ii) Some of the software supporting the ITL system was exposed to continuity risks (i.e., the application server was supported until November 2013; the database was supported until July 2013; and the operating system will reach its end-of-life by July 2015); and

(iii) The servers (i.e., Wintel) were seven years old and may require replacement. They had maintenance contracts in place until 2015.

23. UNFCCC acknowledged the business continuity risks identified during the audit and took action to mitigate these risks by extending the application and database supports, planning for hardware and operating system upgrades.

24. The absence of a complete ITL business continuity plan exposed UNFCCC to the risk of not being able to adequately support ITL in case of unforeseen internal or external events that could negatively impact its operations and support.

(2) UNFCCC should accelerate the completion of its overall business continuity plan. Until such plan is created, UNFCCC should document and establish interim measures for ensuring the continuity of the operations of the International Transaction Log system.

UNFCCC accepted recommendation 2 and stated that it will define compensatory measures by establishing and documenting risks that would impact continuity of the ITL operations. Recommendation 2 remains open pending receipt of evidence showing the measures put in place to ensure the continuity of ITL operations.

There was a need to fill vacant posts

25. The organizational chart of the ITL supporting team provided for a full time P-4 Team Leader, a P-3 Project Manager, a P-3 Service Desk Operations Manager, a P-2 Operations Officer, a G-4 Administrative Assistant, and 50% of a G-6 Information Systems Assistant for vendor management support.

26. The UNFCCC staffing resources for the ITL system were understaffed at the time of the audit. The P-4 Team Leader position was vacant at the time of the audit and had been vacant for more than one year. This function was handled by a staff member working in another section of UNFCCC. However, only 30% of that post's time was allocated to ITL related activities. The position was required to handle critical activities related to vendor management and contractual services.

27. The P-3 Service Desk Operations Manager post was vacant but backfilled by a staff member from another UNFCCC unit. At the time of the audit, this post had not been advertised. According to the information provided by the Office of Human Resources Management, the person who had previously vacated the position was still officially occupying the post, which prevented the post from being advertised. This post was responsible for critical tasks related to change management, monitoring, and vendor compliance.

28. Understaffing of the ITL team exposed UNFCCC to the risk that the ITL system may not be effectively supported to deliver the expected results.

(3) UNFCCC should, as a matter of priority, conduct and complete the recruitment for all the posts allocated to the International Transaction Log system team.

UNFCCC accepted recommendation 3 and stated that the P-4 Team Lead and the P-3 Operations Lead positions in the ITL unit have been filled. Based on the actions taken by UNFCCC, recommendation 3 has been closed.

B. Performance monitoring mechanisms

Systems performance and data centre monitoring mechanisms were adequate

29. Clear terms of reference should be defined and monitored for systems performance and data centre operations. The terms of reference should include metrics and mechanisms to monitor system availability, capability issues, inefficiencies, and expected response and resolution times for support.

30. UNFCCC had documented and implemented the terms and conditions for monitoring the ITL system and data centres. The designated data centres had a 24x7 onsite presence and environment monitoring. There were specialized applications monitoring in real time data for networks, systems and equipment. The monitoring software was configured to provide alerts on problems with any system or equipment, and generated ongoing dashboards with statistics on the performance of the ITL system. This software was able to identify locations of single points of failure. A process was also in place to notify the designated supervisor or manager, should an outage or incident occur. An escalation procedure was in place for incident resolution and documentation. Network monitoring software automatically logged the statistics and reports that were provided to UNFCCC.

31. In the opinion of OIOS, the controls designed and implemented for monitoring the performance of the systems and the data centres supporting the ITL were adequate.

C. Information and communications technology support system

There were weaknesses in security vulnerability assessments

32. Vulnerability assessments and penetration testing should be conducted periodically to determine and evaluate potential security weaknesses in computer systems and networks.

33. Vulnerability assessments and penetration tests of the ITL system were performed annually by a third party service provider. Test results and recommendations to mitigate the risks identified were documented and presented to UNFCCC. However, the third party service provider that performed the vulnerability assessments was hired (subcontracted) by the service provider which was engaged for the operation and support of the ITL system. Therefore, there was an apparent conflict of interest given that the same entity was responsible for operating, supporting, and testing the vulnerability of the ITL system.

34. The vulnerability assessments and penetration tests performed by the third party service provider included web application testing, internal network testing, and firewall reviews. Test results were documented with identified vulnerabilities, potential implications on the ITL system, and recommended corrective actions. The test results included security issues rated critical, important, and medium. A review of the follow-up actions taken by UNFCCC to address the issues identified in the vulnerability assessments indicated that: (i) there were no documented action plans to mitigate the vulnerabilities identified during the penetration test conducted in 2012; (ii) there were still unresolved security issues identified in 2010 and 2011 tests; and (iii) the risks associated with these vulnerabilities were not included in the ITL risk register.

35. Inadequate arrangements for security vulnerability assessments and penetration tests may have a negative impact on the availability, confidentiality, and integrity of the ITL system.

(4) UNFCCC should ensure that: (i) vulnerability and penetration tests of the International Transaction Log system are conducted by entities that are independent from the providers of operational and support services to ITL; (ii) the risks identified during the vulnerability and penetration tests are recorded in a risk register; and (iii) mitigation actions are planned and executed in a reasonable timeframe.

UNFCCC accepted recommendation 4 and stated that: (i) vulnerability and penetration tests of the ITL system are already conducted by an independent entity of the ITL support operator. However, UNFCCC will explore the feasibility of engaging an external provider; (ii) the risks

identified during the vulnerability tests will be recorded for the preparation of the risk management policies; and (iii) appropriate mitigation actions will be planned and executed for the identification and assessment of the risks. Recommendation 4 remains open pending receipt of evidence of the engagement of a third party service provider to perform vulnerability tests of the ITL system; copy of the risk register reflecting the results of vulnerability tests; and the corresponding risk mitigation action plans.

Weaknesses regarding source code verification had been addressed

36. Software source code and subsequent changes must be approved by business owners. The transport of source code from the development to the production environment should also be strictly controlled to ensure the integrity of the authorized code before and after its migration in production.

37. Changes and updates to the ITL source code were performed by the third party service provider, and the software package generated from the source code was moved to production by the third party service provider in charge of operations and support of the ITL system. However, an integrity verification was not performed to ensure that the software package approved by the business owners was the same version as the one moved in production.

38. The lack of a process to ensure the code integrity of the ITL software code presented the risk that the production source code tested and approved may not be the same code as the one deployed and used in production by the registries and UNFCCC. UNFCCC acknowledged the risk and developed a procedure for deployment verification.

39. UNFCCC addressed the control weaknesses identified and provided evidence of the procedure developed for the verification of the source code. In view of the actions taken by UNFCCC, no recommendation was made.

Version control weaknesses needed to be addressed

40. Policies and procedures should be managed with version control mechanisms ensuring that only the final and approved version of the relevant document is referenced and implemented.

41. The ITL system had a large number of documents detailing policies and operational procedures. All policies and operational procedures related to the ITL system were managed with a version control tool hosted and managed by the service provider. Although this tool provided versioning details, it was not intended to be used as a document repository for storing approved documents. There was no indication in the documents identifying them as the final approved versions. Policies and procedures were created and updated by UNFCCC staff, as well as by the third party service provider.

42. The inability to identify the approved versions of the policies and procedures related to the ITL system could lead to users following outdated instructions.

(5) UNFCCC should implement an International Transaction Log system document management policy to ensure adequate identification of the final version of policies and standard operating procedures.

UNFCCC accepted recommendation 5 and documented the policy to ensure that at any given time the final and approved version of each document can be retrieved and used. Based on the actions taken by UNFCCC, recommendation 5 has been closed.

Access control policy was obsolete

43. Access controls should enable the determination of who has access to specific systems and resources at a given time, including mechanisms for identifying, authenticating, and authorizing users.

44. The access control policy of the ITL system was obsolete. The policy was documented in 2007 and contained names of staff members who were no longer part of the ITL team. In addition, there were no compliance tests performed by UNFCCC to ensure that the controls documented in the access control policy were implemented by the third party vendor.

45. Additionally, the logs recording the activity of the administrator of the ITL system were not reviewed periodically by UNFCCC, and automated alerts for critical administrative operations in the application and in the database were not activated. This condition may lead to undetected unauthorized activities in the system.

(6) UNFCCC should: (i) review, update, and approve the International Transaction Log system access control policy; (ii) perform periodic compliance checks on the implementation of the access control mechanisms defined in the policy; (iii) activate the automated alert mechanisms for critical activities performed by the ITL administrator, system administrators and database administrators; and (iv) perform periodic monitoring of the administrator logs.

UNFCCC accepted recommendation 6 and stated that it has reviewed, updated, and approved the ITL access control policy, and commenced periodic monitoring of the ITL administrator application logs as of March 2014. UNFCCC will perform periodic compliance checks to ensure proper implementation of the access control policy, and implement a solution for the automated alert mechanism or define a compensatory manual measure to monitor critical activities. Recommendation 6 remains open pending receipt of evidence of periodic compliance checks of access controls and automated alert mechanisms.

Password controls needed strengthening

46. The use of strong passwords and authentication controls should be in place to lower the risk of a security breach. Policies and procedures related to password security should be implemented and regularly enforced.

47. The password policy for the ITL system required strong passwords. However, this policy was not implemented and enforced with automated controls in the system. The passwords used for access to the ITL system were short passwords and had no expiration dates.

48. The ITL security policy documented by the third party service provider incorrectly indicated that all passwords in use in the ITL system (i.e., ITL Administration Application users and passwords, Registry user names and passwords, console user names and passwords, and database user names and passwords) were stored in the same location in an encrypted Excel file.

49. Weak password controls and outdated password security procedures exposed the ITL system to security risks.

(7) UNFCCC should: (i) implement a strong password policy for all the components of the International Transaction Log system (application, database, and operating system levels); (ii) perform periodic monitoring of the implementation of the password policy on the third

party service provider sites supporting ITL; and (iii) update the ITL security policies.

UNFCCC accepted recommendation 7 and stated that it has updated section 8 of the ITL Security Policy to reflect the actual password management and storage. UNFCCC will: (i) review and assess the components of the ITL system in terms of their compliance with the strong password policy and implement the policy for non-compliant components; and (ii) perform a periodic monitoring of the password policy implementation for the ITL system. Recommendation 7 remains open pending receipt of the password policy and compliance reports showing the implementation of the policy.

Change management procedures were inadequate

50. Change management procedures for system software and ICT infrastructure should be in place to ensure minimal disruption of services and cost effective utilization of resources involved in implementing changes.

51. UNFCCC established a change management procedure since the go-live of the ITL system. This procedure included instructions for performing functional changes to the ITL application and changes to the business procedures related to the ITL system. However, the change management procedure did not cover non-functional changes to the ITL system such as system software and infrastructure related changes. The non-functional changes were required for improving performance, security, quality, and support of the system. These types of non-functional change requirements were partially covered in the meetings of the Steering Group and some changes were discussed in the tracking system by the involved parties. However, these discussions did not present a formal change management process for the non-functional changes of the ITL system (i.e., hardware changes and system software changes such as database and web server).

(8) UNFCCC should revise and implement the International Transaction Log system change management procedure to include changes related to infrastructure, security, and quality.

UNFCCC accepted recommendation 8 and stated that the existing change management process of the non-functional changes has been documented in the ITL system change management procedure. Based on the actions taken by UNFCCC, recommendation 8 has been closed.

Controls over the physical infrastructure and backup operations were adequate

52. Data centres hosting ICT systems should provide a reliable and secure infrastructure environment, in compliance with relevant technical standards, in order to minimize any chances of disruptions.

53. The ITL system was hosted in two data centres (primary and secondary data centres) away from Bonn. Controls over the physical infrastructure at the data centres were found to be adequate on the basis of:

(i) At the primary data centre, there was adequate video surveillance and screening procedures for granting access to the facility;

(ii) There were adequate controls for redundancy of power and cooling systems; and

(iii) The data centre location had a fire alarm system, fire extinguishers, and sprinkler systems in place.

54. The backup data centre had adequate physical controls in place. Strong access control mechanisms were in place, including: (i) identification controls; (ii) advance approvals required for physical access to the site; (iii) airlock entry system (i.e., a small chamber with two airtight doors which did not open simultaneously); and (iv) use of approved escorts required at all times.

55. Adequate controls were also in place for the following mechanisms:

(i) The electronic key process was fully controlled;

(ii) The backup data centre had two power supplies with two divergent distribution paths and load balancing;

(iii) The backup data centre location had an adequate fire alarm system; and

(iv) There was a contract with a service provider for offsite storage of backup tapes. A review of the documented processes and the latest audit reports of the offsite storage facilities showed that the process was adequately supported and the facilities were secure and had adequate environmental controls in place.

Incident and problem management were satisfactory

56. Incidents to critical systems should be resolved as quickly as possible to restore normal service operations within the timeframes specified in predefined service level agreement. Where multiple occurrences of similar incidents continue to happen, a process should be in place to record the event, resolve the problem, and prevent its reoccurrence.

57. The incident and problem management tickets and records related to the ITL system from July 2007 through October 2013 showed an initial trend of several incidents and problems during the earlier years of implementation of the system. The time taken to resolve the incidents did not consistently meet the relevant service level agreement targets. However, over time, there was significant reduction in the number of incidents and improvement in the timeliness of their resolution.

58. There were a total of 9 incidents (down from 17 in 2010) in 2011. Seven of the 9 incidents were resolved in accordance with the targets defined in the relevant service level agreement. In 2012, there were a total of 4 incidents, which were not resolved within the required timeframes defined in the service level agreement. However, during the period January through October 2013 there was only 1 incident and its resolution met the target defined in the service level agreement.

59. OIOS considered the current UNFCCC incident and problem management processes and procedures to be adequate on the basis of the following controls: (a) there was significant reduction in the number of incidents in 2013; (b) there were detailed records of incident and problem resolutions, some resulting in change requests which were implemented; (c) all 2013 incidents met the target defined in the service level agreement; (d) UNFCCC performed ongoing monitoring of the third party vendor's performance through monthly progress reports; and (e) the third party vendor conducted surveys to identify and address service level weaknesses.

IV. ACKNOWLEDGEMENT

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

(*Signed*) David Kanja
Assistant Secretary-General for Internal Oversight Services

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of the International Transaction Log system at the United Nations Framework Convention on Climate Change

Recom. no.	Recommendation	Critical[2]/ Important[3]	C/ O[4]	Actions needed to close recommendation	Implementation date[5]
1	UNFCCC should document and implement a risk management policy for the International Transaction Log system, including formal procedures for risk assessment, risk monitoring, and mitigation plans.	Important	O	Recommendation 1 remains open pending receipt of the risk management policy and procedures describing the risk assessment, monitoring and mitigation processes.	30 September 2014
2	UNFCCC should accelerate the completion of its overall business continuity plan. Until such plan is created, UNFCCC should document and establish interim measures for ensuring the continuity of the operations of the International Transaction Log system.	Important	O	Recommendation 2 remains open pending receipt of evidence showing the measures put in place to ensure the continuity of ITL operations.	30 September 2014
3	UNFCCC should, as a matter of priority, conduct and complete the recruitment for all the posts allocated to the International Transaction Log system team.	Important	C	Action completed.	Implemented
4	UNFCCC should ensure that: (i) vulnerability and penetration tests of the International Transaction Log system are conducted by entities that are independent from the providers of operational and support services to ITL; (ii) the risks identified during the vulnerability and penetration tests are recorded in a risk register; and (iii) mitigation actions are planned and executed in a reasonable timeframe.	Important	O	Recommendation 4 remains open pending receipt of evidence of the engagement of a third party service provider to perform vulnerability tests of the ITL system; copy of risk register reflecting results of vulnerability tests; and risk mitigation action plans.	31 December 2014
5	UNFCCC should implement an International Transaction Log system document management	Important	C	Action completed.	Implemented

[2] Critical recommendations address significant and/or pervasive deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance cannot be provided regarding the achievement of control and/or business objectives under review.
[3] Important recommendations address important deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.
[4] C = closed, O = open
[5] Date provided by UNFCCC in response to recommendations.

ANNEX I

STATUS OF AUDIT RECOMMENDATIONS

Audit of the International Transaction Log system at the United Nations Framework Convention on Climate Change

Recom. no.	Recommendation	Critical[2]/ Important[3]	C/ O[4]	Actions needed to close recommendation	Implementation date[5]
	policy to ensure adequate identification of the final version of policies and standard operating procedures				
6	UNFCCC should: (i) review, update, and approve the International Transaction Log system access control policy; (ii) perform periodic compliance checks on the implementation of the access control mechanisms defined in the policy; (iii) activate the automated alert mechanisms for critical activities performed by the ITL administrator, system administrators and database administrators; and (iv) perform periodic monitoring of the administrator logs	Important	O	Recommendation 6 remains open pending receipt of evidence of the periodic compliance checks of access controls and automated alert mechanisms.	30 September 2014
7	UNFCCC should: (i) implement a strong password policy for all the components of the International Transaction Log system (application, database, and operating system levels); (ii) perform periodic monitoring of the implementation of the password policy on the third party service provider sites supporting ITL; and (iii) update the ITL security policies	Important	O	Recommendation 7 remains open pending receipt of password policy and compliance reports showing the implementation of the policy.	31 December 2014
8	UNFCCC should revise and implement the International Transaction Log system change management procedure to include changes related to infrastructure, security, and quality.	Important	C	Action completed.	Implemented

APPENDIX I

Management Response

United Nations Nations Unies

INTEROFFICE MEMORANDUM MEMORANDUM INTERIEUR

TO: Mr. Gurpur Kumar, Deputy Director DATE: 22 April 2014
A: Internal Audit Division, Office of Internal Oversight Services

THROUGH: Mr. Richard Kinley, Deputy Executive Secretary
S/C DE: United Nations Framework Convention on Climate Change

FROM: Claribelle Poujol, Manager, IMM sub-programme, ITS
DE: United Nations Framework Convention on Climate Change

SUBJECT: **The United Nations Framework Convention on Climate Change's**
OBJET: **comments on the draft audit report:**
Assignment No. AT2013/241/01 – Audit of the International Transaction Log

1. With reference to the above subject and in response to your memorandum dated 8 April 2014 addressed to Mr. Richard Kinley, Deputy Executive Secretary, UNFCCC, please find attached the action plan to address the recommendations issued in the report as well as supporting documentation and comments pertaining to the recommendations.

2. Thank you for the opportunity to provide our comments. We are at your disposal for any further information or clarifications.

Kind regards.

cc: Mr. James Grabert, Officer-In-Charge, ITS, UNFCCC
Ms. Marites Sese, OIOS Resident Auditor, UNFCCC
Ms. Anna Halasan, Professional Practices Section, Internal Audit Division, OIOS
Mr. Hinko Vincar, ITL Team Lead, ITS, UNFCCC

APPENDIX I

Management Response

Audit of the International Transaction Log system at the United Nations Framework Convention on Climate Change

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
1	UNFCCC should document and implement a risk management policy for the International Transaction Log system, including formal procedures for risk assessment, risk monitoring, and mitigation plans.	Important	Yes	Manager, IMM sub-programme	30 September 2014	UNFCCC will document and implement a risk management policy for the ITL system, including formal procedures for risk assessment, risk monitoring, and mitigation plans.
2	UNFCCC should accelerate the completion of its overall business continuity plan. Until such plan is created, UNFCCC should document and establish interim measures for ensuring the continuity of the operations of the International Transaction Log system.	Important	Yes	Manager, IMM sub-programme	30 September 2014	UNFCCC will define compensatory measures by establishing and documenting risks that would impact continuity of the ITL operations. In regard to the risks identified in the report and that could negatively affect UNFCCC's ability to ensure the continuity of the ITL system, please note the following: **i)** The business impact analysis on the possible transition of the ITL services is a part of the future plan to evaluate the current arrangements and to decide on the options including extending the original contract. **UNFCCC requests removing the finding from**

[1] Critical recommendations address significant and/or pervasive deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance cannot be provided regarding the achievement of control and/or business objectives under review.
[2] Important recommendations address important deficiencies or weaknesses in governance, risk management or internal control processes, such that reasonable assurance may be at risk regarding the achievement of control and/or business objectives under review.

APPENDIX I

Management Response

Audit of the International Transaction Log system at the United Nations Framework Convention on Climate Change

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
						the audit report. **ii)** The application server support has been extended until the end of 2014. The database support has been extended until April 2015. Similarly, the upgrade of the operating system is a general practice planned under operational policies and will be completed before its end-of-life. **UNFCCC requests removing the finding from the audit report.** iii) The renewal of the servers is a general practice planned under hardware replacement policies and will be completed before the expiration of the maintenance contracts. **UNFCCC requests removing the finding from the audit report.**
3	UNFCCC should, as a matter of priority, conduct and complete the recruitment for all the posts allocated to the International Transaction Log system team.	Important	Yes	Coordinator, ITS programme	Implemented	UNFCCC has implemented this recommendation. The P-4 Team Lead and the P-3 Operations Lead positions in the ITL unit have been filled.

APPENDIX I

Management Response

Audit of the International Transaction Log system at the United Nations Framework Convention on Climate Change

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
4	UNFCCC should ensure that: (i) vulnerability and penetration tests of the International Transaction Log system are conducted by entities that are independent from the providers of operational and support services to ITL; (ii) the risks identified during the vulnerability and penetration tests are recorded in a risk register; and (iii) mitigation actions are planned and executed in a reasonable timeframe.	Important	Yes	Team Lead, ITL unit	31 December 2014	(i) Vulnerability and penetration tests of the ITL system are already conducted by an independent entity of the ITL support operator; however, UNFCCC will explore feasibility of engaging an external provider; (ii) the risks identified during the vulnerability tests will be recorded upon the preparation of the risk management policies; and (iii) appropriate mitigation actions will be planned and executed upon identification and assessment of the individual risks.
5	UNFCCC should implement an International Transaction Log system document management policy to ensure adequate identification of the final version of policies and standard operating procedures.	Important	Yes	Team Lead, ITL unit	Implemented	UNFCCC has implemented this recommendation. The document management policy to ensure adequate identification of the final version of policies and standard operating procedures for the ITL system was defined and implemented.
6	UNFCCC should: (i) review, update, and approve the International Transaction Log system access control policy; (ii) perform periodic compliance checks on the implementation of the access control mechanisms defined in the policy; (iii) activate the automated alert mechanisms for critical activities performed by the ITL administrator, system administrators and database administrators; and (iv) perform periodic monitoring of the administrator	Important	Yes	Team Lead, ITL unit	Parts (i) and (iv) are implemented Part (ii) and (iii) will be implemented by 30 September 2014	UNFCCC has: (i) reviewed, updated, and approved the ITL access control policy; and (iv) commenced periodic monitoring of the ITL administrator application (ITL-AA) logs as of March 2014. UNFCCC will: (ii) perform periodic compliance checks to ensure proper implementation of the access control policy; and (iii) implement a solution

APPENDIX I

Management Response

Audit of the International Transaction Log system at the United Nations Framework Convention on Climate Change

Rec. no.	Recommendation	Critical[1]/ Important[2]	Accepted? (Yes/No)	Title of responsible individual	Implementation date	Client comments
	logs.					for the automated alert mechanism or define a compensatory manual measure to monitor critical activities.
7	UNFCCC should: (i) implement a strong password policy for all the components of the International Transaction Log system (application, database, and operating system levels); (ii) perform periodic monitoring of the implementation of the password policy on the third party service provider sites supporting ITL; and (iii) update the ITL security policies.	Important	Yes	Team Lead, ITL unit	Part (iii) is implemented Parts (i) and (ii) will be implemented by 31 December 2014	UNFCCC has (iii) updated the Section 8 of the ITL Security Policy to reflect the actual password management and storage. UNFCCC will: (i) review and assess the components of the ITL system in terms of their compliance to the strong password policy and implement the policy for non-compliant components; and (ii) perform a periodic monitoring of the password policy implementation for the ITL system.
8	UNFCCC should revise and implement the International Transaction Log system change management procedure to include changes related to infrastructure, security, and quality.	Important	Yes	Team Lead, ITL unit	Implemented	UNFCCC has implemented this recommendation. The existing change management process of the non-functional changes has been documented in the ITL system change management procedure.